CURRENT TECHNIQUES, PRACTICES, AND INSTRUMENTS OF MONEY LAUNDERING AND TERRORISM (SEPARATISM) FINANCING

2021

The State Financial Monitoring Service of Ukraine

The State Financial Monitoring Service of Ukraine

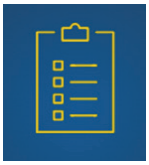
CURRENT TECHNIQUES, PRACTICES, AND INSTRUMENTS OF MONEY LAUNDERING AND TERRORISM (SEPARATISM) FINANCING

Kyiv 2021

The State Financial Monitoring Service (SFMS) has been established as the financial intelligence unit (FIU) tasked with counteracting to money laundering and financing of terrorism.

The SFMS is the FIU of the so-called «administrative type».

The key role of the SFMS is to process suspicious transaction reports obtained from reporting entities and forward case referrals to Ukrainian law enforcement and intelligence agencies if ML/TF/PF suspicions arise.



More information about the SFMS is available online:
fiu.gov.ua

Link to typologies studies undertaken by the SFMS:
fiu.gov.ua/pages/dijalnist/tipologi

EUACI EUROPEAN UNION ANTI-CORRUPTION INITIATIVE

The collection was implemented with the support of the EU Anti-Corruption Initiative (EUACI)

APPROVED
by Order of the State Financial
Monitoring Service of Ukraine
of December 20, 2021 No. 146

Typological study on:
"Current Techniques, Practices, and Instruments of Money Laundering and Terrorism (Separatism) Financing"

This typological study explores issues relating to detection, disclosure and investigation of current money laundering and terrorism (separatism) financing schemes. It also covers the substance and characteristics of various schemes employed to launder money and commit other crimes.

The study sheds light on the techniques, practices, and instruments of money laundering and terrorism (separatism) financing as well as on indicators used to detect those involved in illegal schemes.

The crucial role of the risk-based approach in controlling such crimes is highlighted.

This typological study can lay the groundwork for measuring the level of suspicion aroused by a financial transaction or money laundering activities as well as other crimes.

CONTENTS

LIST OF ABBREVIATIONS

SFMS	The State Financial Monitoring Service of Ukraine
ML/TF/PF	Money laundering, terrorist financing, and financing of the proliferation of weapons of mass destruction
AML/CFT	Anti-money laundering/ counter-terrorist financing
UBO	Ultimate beneficial owner
CC of Ukraine	Criminal Code of Ukraine
NPO	Non-profit organization
FIU	Financial intelligence unit of a foreign state
BE	Business entity
IE	Individual entrepreneur
FATF	Financial Action Task Force

FOREWORD

This typological study reflects the current schemes employed in money laundering and financing of terrorism (separatism) and other crimes.

The experience of recent years has made it possible to structure schemes according to the most common categories of cases that gave rise to financial investigations.

Specifically, the SFMS has undertaken typological studies focusing on the following relevant topics in recent years: Money laundering of tax crimes (2020), Misappropriation of funds and assets of state-owned enterprises and other entities funded from the state and local budgets (2019), Risks of using opaque ownership structures in money laundering (2018), Risks of cash use (2017), Risks of terrorism and separatism (2017), Money laundering from corruption (2016), etc.

Typological studies of the SFMS have enabled reporting entities to formulate an understanding of risks and improve their practices of using the risk-based approach.

Overall, it is worth noting that while money laundering and terrorist financing typologies are evolving rapidly, the understanding of the highlighted schemes by the AML/CFT system participants has made it possible to take the appropriate measures for potential harm mitigation.

Bearing in mind the adverse economic impact of criminal proceeds generated in various sectors as a result of different crimes, the SFMS has chosen the relevant topic covering the latest trends in the schemes employed by criminals.

INTRODUCTION

Since the start of 2020, the COVID-19 pandemic has affected not only citizens and economic processes in the state, but also the ML/TF/PF schemes used.

The COVID-19 pandemic has prompted certain changes in economic processes as regards the application of the latest advanced technologies in financial practices, which has in turn opened up new opportunities for criminals to commit economic crimes and generate illicit proceeds.

Cases involving various types of fraud, cybercrimes, and the use of the latest technologies to commit them have substantially increased.

In this context, it is only logical that the SFMS is working actively to study and launch financial investigations into the following cases:

a) laundering of proceeds from corruption crimes;
b) laundering of proceeds from embezzlement and misappropriation of public funds and resources of state-owned business entities;
c) laundering of proceeds from tax crimes;
d) investigation of cases involving terrorism and separatism financing;
e) money laundering through the insurance and securities markets;
f) laundering of proceeds from arms trade;
g) laundering of proceeds from drug and psychotropic substances trade;
h) laundering of proceeds from human trafficking and distribution of pornographic video;
i) laundering of proceeds from fraud;
j) laundering of proceeds from cybercrimes;
k) commission of crimes and money laundering with the use of virtual assets.

The goal of this study is to analyze and summarize ML/TF/PF instruments, indicators, and techniques.

This typological study uses the practices of the national financial monitoring system participants.

CHAPTER I.
GENERAL TRENDS

1.1. Threats and risks of illicit financial transactions

The state's economic security is instrumental to its national security and is closely intertwined with all economic processes occurring in society.

Money laundering crimes are committed not only to subsequently use the proceeds in economic activities to generate income or for self-enrichment, but also for financing terrorism, illicit arms trafficking, organizing contract murders, financing separatist groups and other crimes.

Ukraine has been facing a constant threat of terrorism and separatism in recent years. The use of the financial system for integration and rerouting of financial flows used to support such criminal activities presents a challenge for the state.

Economic crimes in Ukraine demonstrate increasingly more sophisticated ML/TF schemes. Specifically, there are cases of large-scale misappropriation of public funds on a mass, manifestations of corruption, siphoning of capital into foreign jurisdictions, conversion centers ("twists") activity, fraud, tax evasion, concealment of the actual owners of investment projects in the most profitable sectors of the economy, etc.

The spread of the shadow economy and growing organized crime greatly undermine Ukraine's economic security.

Detecting and dismantling money laundering and terrorist financing schemes calls for dedicated efforts of reporting entities and law enforcement agencies that detect and investigate economic crimes.

Between May 2020 and September 2021, the SFMS received 37,728 suspicious financial transaction (activity) reports from reporting entities (vs. 11,465 in 2020 and 25,763 in 2021).

It is noteworthy that in 2020, just like in 2021, more than 50% of suspicious transactions and cases were reported based on the "other indicators" attribute, meaning that reporting entities identified other suspicions. Practical analysis of such reports and cases indicates that they involve business entities showing signs of being fictitious, while their transactions are "transit in nature" undertaken to "provide services" conducive to tax evasion by employing the mechanism of "counter flows", "twists" followed by cash-out practices.

A substantial number of cases reported in 2021 were also based on suspicions of "conversion of non-cash funds into cash", "financial transactions involving assets that do not match the customer's profile", "fictitious entrepreneurship", and "fraud".

The overwhelming majority of transactions and cases (80%) involve tax evasion schemes.

1.2. Risks of involvement of business entities in ML/TF/PF in a breakdown by activity

Depending on their business, various entities have different levels of risk of involvement in ML/TF/PF. Detailed information about probable risk level is provided in the table.

Level of risk of various entities depending on their activity[1]

Section	A	Description of activity	Agriculture, forestry, and fishery
Risks associated with activity	The risk factor inherent in these activities involves the use of large amounts of cash to pay contracting parties. It is also difficult to monitor actual volumes of production, cultivation and sales. This factor substantially complicates monitoring and keeping track of payments with each particular business entity. Proof of payment is nonexistent in many instances. This business also permits keeping produce off the books by underreporting the actual output volumes. Possible risks: • exports without repatriation of earnings or marketing of products of unknown origin. Various estimates indicate that a substantial share of cropland is cultivated off the books and without payment of taxes.		

Section	B	Description of activity	Mining industry and quarry development
Risks associated with activity	This activity involves the extraction of minerals. The actual output volumes are difficult to keep track of. Business entities engaged in this activity are able to conceal the actual output of minerals, keep them off the books, and sell them unofficially thereby evading taxes. Possible risks: • misappropriation of a substantial share of minerals extracted; • understatement of taxes payable upon the sale of minerals as well as mineral extraction taxes; • mining for minerals without obtaining a permit.		

1 Source: results of surveys of reporting entities and law enforcement agencies

Section	C	Description of activity	Processing industry
Risks associated with activity	Entities are able to keep their production off the books by purchasing raw materials with cash and underreporting output volumes. There is also the risk of overstatement of costs as a way to evade taxes. Possible risks: • manufacture and sale of products off the books; • procurement of a substantial share of raw materials from IE operating under the simplified taxation system (opportunities for conversion); • declaration of tax credit from business entities that show signs of being "fictitious".		

Section	D	Description of activity	Supply of electricity, gas, steam, and conditioned air
Risks associated with activity	The following risks are inherent in this activity: it is difficult to quantify consumer demand; market players resort to manipulations; market competition is imperfect (tariffs are set in a nontransparent manner); it is not possible to monitor performance of obligations by contracting parties. Possible risks: • illicit proceeds from energy utilization schemes; • declaration of tax credit from business entities that show signs of being "fictitious"; • business dealings with IE operating under the simplified taxation system (opportunities for conversion from mon-cash funds into cash).		

Section	E	Description of activity	Water supply, wastewater disposal, waste management
Risks associated with activity	Noteworthy risks in this area include: a nontransparent system of payments for services rendered; lack of effective control over companies in the housing and utility sector; inability to monitor performance of obligations by contracting parties.		

Section	F	Description of activity	Construction
Risks associated with activity	While this industry is highly profitable, business entities in this sector need to incur substantial "unofficial costs" in order to succeed. In turn, this necessitates taking cash flows off the books, which results in tax evasion. Construction involves using substantial quantities of resources (construction materials), which allows business entities to overstate the actual consumption of resources thereby over reporting gross expenditure and evading taxes. It is also worth mentioning: a high level of corruption in the construction industry; possible misspending of funds; unscrupulous developers and fraudulent schemes; reliance on a large number of subcontractors; lack of effective control. Possible risks: • tax evasion and money laundering in construction with the use of co-investment mechanisms; • registering the sale of apartments through citizens who are not officially registered as business entities; • misappropriation of public funds allocated for targeted funding programs; • declaration of tax credit from business entities that show signs of being "fictitious".		

Section	G	Description of activity	Wholesale and retail, car and motorcycle servicing
Risks associated with activity	Wholesale businesses can be used for "transit" transactions and accumulation of tax credit. Major retailers can act as "cash sellers". Risk factors in this industry: large quantities of cash in circulation; use of tax evasion schemes that rely on mechanisms of "transit", "twists"; fictitious entrepreneurship; illicit foreign exchange transactions under fictitious foreign trade contracts; large number of parties to financial transactions; high percentage of the shadow economy; pseudo-import operations; reporting sales through IE operating under the simplified taxation system as a way to minimize official income; illicit trade in excisable goods; envelope wages; using cash for business transactions; "sale" of tax credit to entities in the real sector of the economy as a way to minimize taxes. In the retail market, goods that entered Ukraine or were produced domestically without the payment of taxes are sold using the following schemes: • fully illegal clandestine trade, whereby goods are sold without payment of any taxes and without any official records. This scheme is used on a mass scale to sell tobacco products; • trade at stores, kiosks, filling stations and similar outlets that are officially registered (as LLC or IE), whereby only a portion of goods are sold via the cash register, while the remaining goods are sold without printing a sales receipt or with the issuance of a fake sales receipt. This scheme is used on a mass scale to sell alcohol, tobacco products, fuel and lubricants; • remote trade in alcoholic beverages via the Internet without using a cash register and without reflecting the actual sales volumes in declarations.		

Section	H	Description of activity	Transportation, warehousing, postal and courier services
Risks associated with activity	Costs can be overstated with the help of transportation and warehousing companies. A common method involves concealing the import of commercial shipments of goods into the customs territory of Ukraine as postal or courier deliveries under the guise of personal imports or carriage of personal belongings, whereby individuals transport goods in carry-on luggage or accompanied luggage (a large shipment of goods is split among an established group of several dozen or even hundred individuals (most commonly residents of frontier areas) into shipments that can be imported free of charge; once they cross the border on foot or in cars or buses, the goods are collected in one place and then transported to various parts of the country).		

Section	I	Description of activity	Temporary lodging and food catering
Risks associated with activity	This business enables entities to keep their production off the books by purchasing raw materials with cash and underreporting output volumes. Risk factors: large amounts of cash in circulation; large number of business entities; complexity of proper monitoring of the scope of services provided; unofficial employment of workers and payment of envelope wages.		

Section	J	Description of activity	Information and telecommunications
Risks associated with activity	This type of activity is difficult to control. One example is public collection of charitable donations with the use of telecom messages.		

Section	K	Description of activity	Financial and insurance services
Risks associated with activity	This category unites financial and insurance companies that can facilitate tax evasion with the aid of instruments commonly used in this sector (for instance, debt assignment agreements, loan agreements, factoring agreements, reinsurance agreements, securities, and so forth). Examples of possible involvement of financial and insurance companies in ML schemes: • pseudo insurance and/or reinsurance; • fictitious insurance claims; • tax and revenues evasion; • instances where insurance companies receive premiums to cover low-probability perils and transfer insurance payouts to shell companies; • reinsurance operations among a large number of affiliated insurance companies without income reporting; • transfers of large amounts by insurance companies to IE under sham agency agreements; • loans extended by financial and banking institutions to affiliated borrowers; • business relations with presumably shell companies; • removing assets out of the collateral pool by transferring title to such assets to third parties; • unjustified use of financial aid operations.		

Section	L	Description of activity	Immovable property transactions
Risks associated with activity	Understatement of actual prices as a way to minimize taxes: immovable property has book (balance sheet) value and market value; this enables business entities to sell immovable property at its book value (that is usually lower than the market value) and conceal the actual income from the sale as a way to avoid taxes. It is also worth mentioning: speculative purchase and sale transactions; large quantities of cash in circulation; legal ignorance of the majority of Ukrainians.		

Section	M	Description of activity	Professional, academic, and engineering activities
Risks associated with activity	The workforce can be employed unofficially (payment of envelope wages).		

Section	N	Description of activity	Administrative and auxiliary services
Risks associated with activity	The workforce can be employed unofficially (payment of envelope wages).		

Section	O	Description of activity	Public administration and defense; mandatory social insurance
Risks associated with activity	A high level of risk is present in the defense sector because it involves large amounts of funding out of the state budget. Unscrupulous officials and business entities take advantage of this by embezzling public funds through questionable tenders, overstatement of prices, etc. When it comes to construction of large-scale infrastructure facilities, this creates opportunities for illicit income in the form of bribes. Overall, it is worth noting: a high level of corruption among public officials and politically significant persons. There is also the risk of misspending of funds allocated from the state and local budgets.		

Section	P	Description of activity	Education
Risks associated with activity	Risks in this sector may be compounded by: endemic corruption; inadequate level of openness and transparency.		

Section	Q	Description of activity	Healthcare and welfare services
Risks associated with activity	Opportunities for corrupt practices exist in the context of tenders staged by enterprises under state or community ownership to procure equipment or medicines, as well as the risk of so-called kickbacks received by public officials. Risks in this sector may be compounded by: endemic corruption; inadequate level of openness and transparency; embezzlement of public funds; various illicit practices (falsification, document forgery). There is a risk of misappropriation of public funds through overstatement of expenses for procurement of goods, work, or services.		

Section	R	Description of activity	Art, sports, entertainment and recreation
Risks associated with activity	One form of this activity involves providing "organized gambling services", which is a highly profitable industry that may provoke unscrupulous entities to seek out tax evasion opportunities. Risks in this sector may also be compounded by: cash transactions; operations of illegal travel agencies; unofficial employment.		

Section	S	Description of activity	Rendering other services
Risks associated with activity	The biggest risk is posed by services that are difficult to quantify and verify whether or not they have been provided (market research, marketing, legal, and other services). There are multiple cases where services are provided fictitiously or at over-inflated prices, making it possible to overstate expenses and evade taxes. Risks in this sector may also be compounded by: cash transactions, unofficial employment, inadequate level of openness and transparency.		

Section	T	Description of activity	Operation of households
Risks associated with activity	There is a potential risk of nonpayment of taxes to state and local budgets following the sale of goods, work, or services produced or provided by households. Risks in this sector may also be compounded by: cash transactions; unofficial employment, inadequate level of openness and transparency.		

The abovementioned risks specific to different activities can help in the assessment of the risks present in the customers' transactions of reporting entities.

CHAPTER II. OVERVIEW OF TRENDS REPORTED BY INTERNATIONAL ORGANIZATIONS AND STUDIES UNDERTAKEN

2.1. FATF on COVID-19 and Measures to Combat Illicit Financing

The members of the FATF, both domestically and multilaterally, are applying every available resource to combat the COVID-19 pandemic.

The FATF encourages governments to work with financial institutions and other businesses to use the flexibility built into the FATF's risk-based approach to address the challenges posed by COVID-19 whilst remaining alert to new and emerging illicit finance risks.

The FATF encourages the fullest use of responsible digital customer on boarding and delivery of digital financial services in light of social distancing measures.

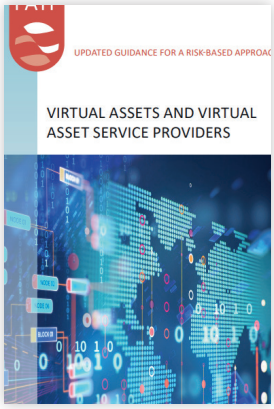
Criminals are taking advantage of the COVID-19 pandemic to carry out financial fraud and exploitation scams, including advertising and trafficking in counterfeit medicines, offering fraudulent investment opportunities, and engaging in phishing schemes that prey on virus-related fears.

Numerous criminals are attempting to profit from the pandemic by exploiting people in urgent need of care and the goodwill of the general public and spreading misinformation about COVID-19.

Like criminals, terrorists may also exploit COVID-19 to amass assets by taking advantage of gaps and weaknesses in national AML/CFT systems.

2.2. Overview of Studies

International organizations have undertaken a number of studies focusing on issues of money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction.

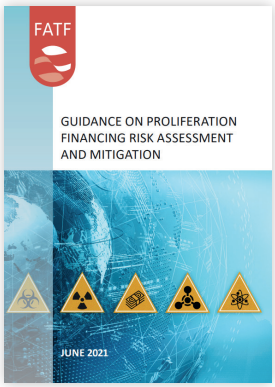


Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers

https://bit.ly/3yDsZiV

Update: COVID-19-related Money Laundering and Terrorist Financing Risks

https://bit.ly/3sTwmzn

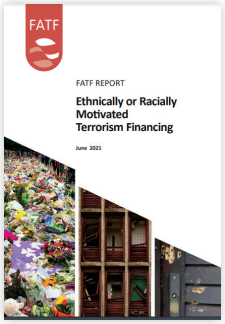


Guidance on Proliferation Financing Risk Assessment and Mitigation

https://bit.ly/3q9BJcZ

Terrorist Financing Risks Assessment Guidance

https://bit. ly/3jjG0rV



Ethnically or Racially Motivated Terrorism Financing

https://bit. ly/3D1HQ7C

Money Laundering from Environmental Crime

https://bit. ly/3BmVvG1

Trade-Based Money Laundering: Risk Indicators

https://bit. ly/3gCJLHv

CHAPTER III. MONEY LAUNDERING TYPOLOGIES

The findings of financial studies indicate that looking to profit from the COVID-19 pandemic criminals have stepped up their efforts in committing economic crimes, especially so when it comes to ML/TF.

In a general sense, money laundering involves taking money obtained from illicit activities and send it through a series of transactions in order to mask its origin and integrate it into the financial system to be subsequently used in the interests of criminals.

The shadow economy has grown in recent years, primarily due to the complex and unusual conditions for doing business during the COVID-19 pandemic.

As new products and technologies evolve, the financial sector offers criminals new practices for remote commission of crimes in both the physical world and the virtual world.

The principal factors behind the transformation of financial crimes are the transition of the global economy to a new technological paradigm, informatization of society in all areas, globalization, and use of different jurisdictions for money laundering.

The SFMS continues its close cooperation with reporting entities, public authorities, and law enforcement agencies aimed at identifying suspicious financial transactions and illegal practices by individuals and legal entities.

The SFMS devotes particular attention to the analysis of suspicious transactions that show signs of money laundering and terrorism (separatism) financing.

In 11 months of 2021, the SFMS transferred **1,091** referrals to law enforcement agencies (including 717 case referrals and 374 additional case referrals).

In these referrals, the grand total of financial transactions that may involve money laundering or criminal activity comes to **UAH 92.7 billion**.

In 2020, the SFMS transferred **1,036** cases to law enforcement agencies (including 607 case referrals and 429 additional case referrals). In these referrals, the grand total of financial transactions that may involve money laundering or criminal activity comes to **UAH 76.2 billion**.

In the 11 months of 2021, the Prosecutor's General Office recorded the following specific crimes:

Number of criminal proceedings	Article of the Criminal Code of Ukraine
18	Article 209 "Legalization (laundering) of the proceeds of crime" of the Criminal Code of Ukraine
295	Article 258 "Act of terrorism" of the Criminal Code of Ukraine
1	Article 258^1 "Involvement in the commission of an act of terrorism" of the Criminal Code of Ukraine
4	Article 258^2 "Public calls inciting the commission of an act of terrorism" of the Criminal Code of Ukraine
125	Article 258^3 "Creation of a terrorist group or a terrorist organization" of the Criminal Code of Ukraine
1	Article 258^4 "Facilitation of the commission of an act of terrorism" of the Criminal Code of Ukraine
34	Article 258^5 "Financing of terrorism" of the Criminal Code of Ukraine

The Prosecutor's General Office has not documented any crimes punishable under Article 439 "Application of weapons of mass destruction".

The most graphical examples of ML/TF are provided below. Refer to the appendix for helpful links where you can find additional information about individuals or legal entities.

3.1. Laundering of proceeds from corruption crimes

Corruption is one of the most dangerous threats to both society and the state as a whole. Corruption in particular directly impacts social development and progress, economic and national security of Ukraine, the investment climate and international image.

Efforts are currently underway in Ukraine to prevent and combat corruption. However, as before, the biggest corruption schemes are typically perpetrated by public officials or executives of enterprises under state or community ownership.

The most common kinds of corruption crimes are: bribery, embezzlement of public funds, forgery in office, abuse of power or office.

Public officials or executives of state- or community-owned enterprises use various schemes to conceal proceeds from corruption crimes.

Common examples relating to corruption crimes are summarized below.

Example 3.1.1.

Money laundering by an executive of a state-owned enterprise

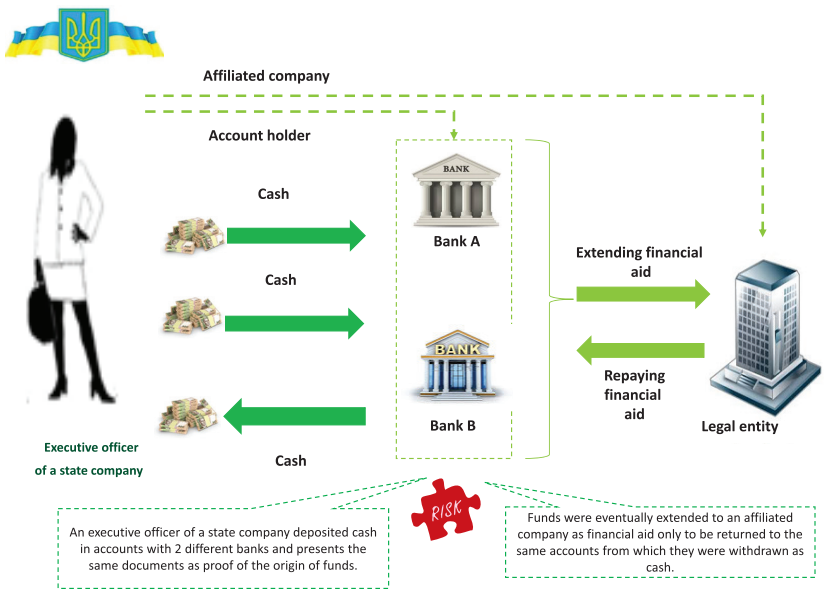
In the course of a financial investigation, the SFMS exposed a scheme used to conceal proceeds from crime.

It was established that an **executive of a state-owned enterprise** deposited millions in cash in current accounts with two different financial institutions.

The funds were subsequently transferred as the financial aid to a legal entity affiliated with this executive of the **state-owned enterprise**. After some time, the legal entity returned the financial aid to the accounts of the executive of the **state-owned enterprise**. The funds were withdrawn as cash.

The executive of the **state-owned enterprise** submitted the same documents to different banking institutions as proof of the origin of cash funds.

The law enforcement agency is conducting a pretrial investigation.



Example 3.1.2.

Money laundering by the family members of a national politically exposed person through investment in costly assets

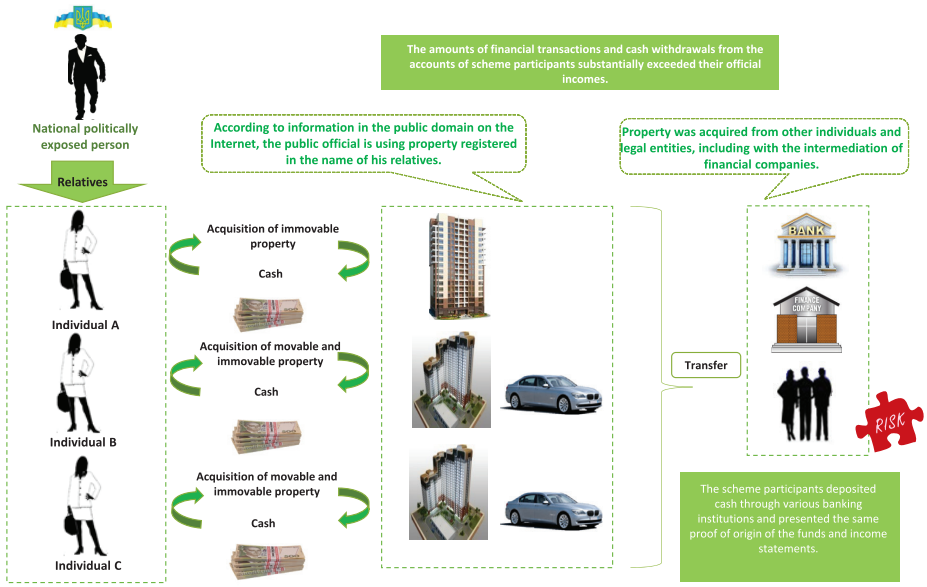
A joint investigation by a law enforcement agency and the SFMS exposed a scheme used to conceal sources of illicit income.

The financial investigation revealed that the **family members of a national politically exposed person** acquired movable and immovable property. Meanwhile, open sources on the Internet helped establish that this property was used by the **national politically exposed person** himself.

The property was bought from other individuals or legal entities and financial companies with cash. The scheme participants deposited cash through various banking institutions and presented the same proof of origin of the funds.

Notably, the amounts of financial transactions and cash withdrawals from the accounts of scheme participants substantially exceeded the incomes declared by them. This could mean that the financial transactions were aimed at money laundering (use of funds originating from unconfirmed sources).

The law enforcement agency is conducting a pretrial investigation.



Example 3.1.3.

Money laundering by the family member of a national politically exposed person through formation of the charter capital

In the course of a financial investigation, the SFMS exposed a scheme used to conceal allegedly illicit income.

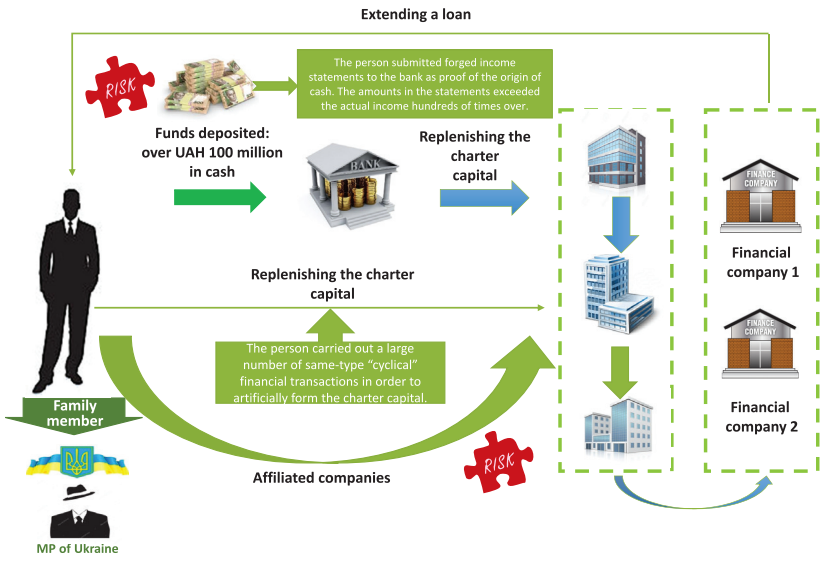
It was established that a **member of the family of a national politically exposed person** deposited over UAH 100 million in cash in their own bank account.

The fact that caught the investigators' attention is that the person submitted forged income statements to the bank as proof of the origin of cash. The amounts in the statements exceeded by hundreds of times the income officially earned by the **family member of a national politically exposed person**.

The funds were subsequently transferred to an enterprise controlled by the **family member of a national politically exposed person** as a contribution to the charter capital. The funds were subsequently rerouted to affiliated legal entities and the cycle was completed as these funds (combined with other funds) were returned to the **family member of a national politically exposed person**.

The funds were subsequently transferred to the account of the affiliated enterprise again. Overall, the person carried out a large number of same-type "cyclical" financial transactions in order to artificially form the charter capital.

The law enforcement agency is conducting a pretrial investigation.



Example 3.1.4.

Money laundering by the family member of a former official through acquisition of title to property

Following a financial investigation, the SFMS exposed a scheme used to conceal sources of allegedly illicit income.

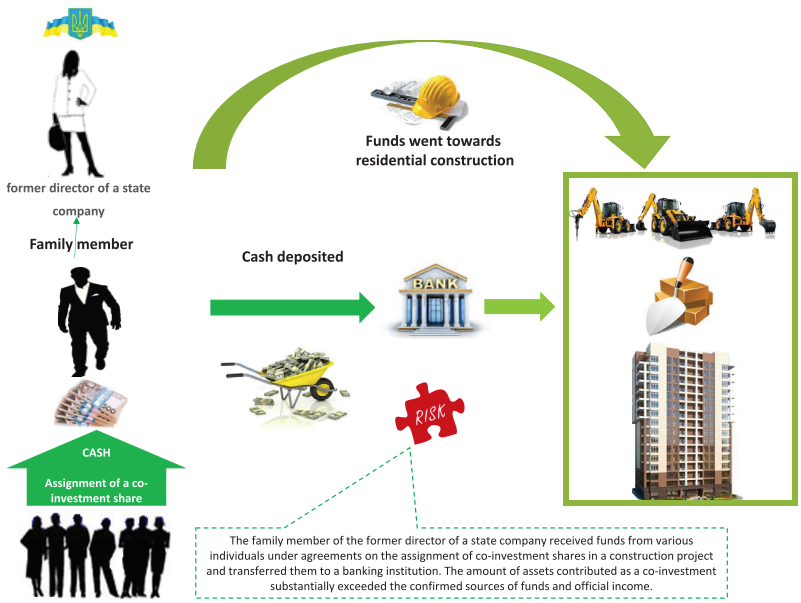
It was established that the family member of a **former executive of a State-owned enterprise** deposited substantial amounts of cash in the account of a housing cooperative as payment of a co-investment contribution.

As proof of the origin of funds, the person presented documents showing receipt of funds from various individuals under agreements on the assignment of co-investment shares in a construction project.

The amount of assets contributed as a co-investment in the housing cooperative substantially exceeded the amount of funds received from such individuals.

The family member of a **former executive of a State-owned enterprise** carried out financial transactions and legal transactions involving assets that substantially exceeded their official income and other confirmed sources (funds received from individuals).

The law enforcement agency is conducting a pretrial investigation.



3.2. Laundering of proceeds from embezzlement and misappropriation of public funds and resources of state-owned business entities

In light of their substantial amounts, public funds allocated to finance the operations of state-owned enterprises, territorial communities (united territorial communities) and other entities funded out of the state or local budget represent a very tempting source of illicit income.

A sizable portion of public funds is currently being allocated for road repairs under the "Large Construction" programme. Significant procurements are also being funded out of the budget in the defense sector and healthcare (procurement of medicines and equipment to combat the COVID-19 pandemic), which gives rise to risks of corruption and embezzlement of public funds.

These risks tend to become increasingly more common as controls over government procurement are loosened.

Listed below are summaries of typical examples of laundering of proceeds from embezzlement and misappropriation of public funds and resources of state-owned business entities.

Example 3.2.1.

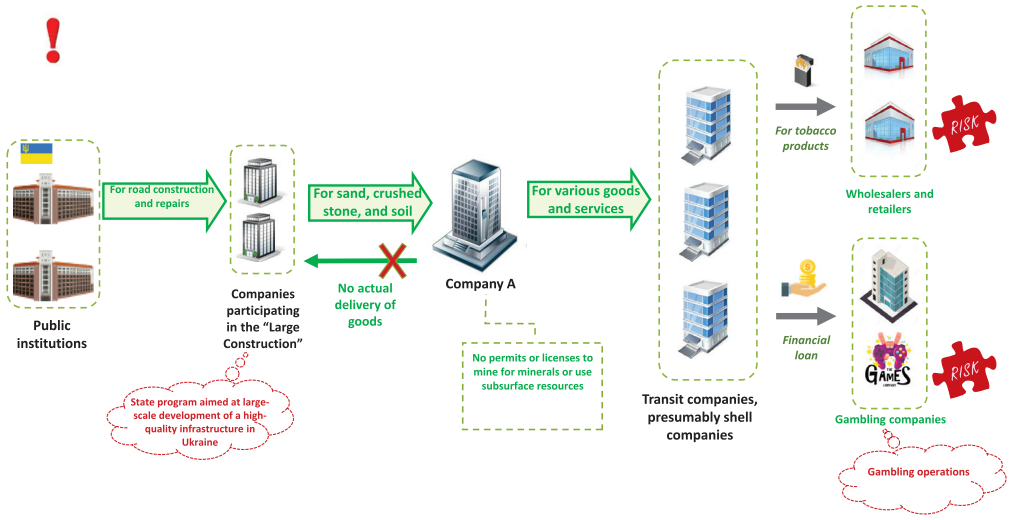
Laundering of proceeds from embezzlement of public funds with the use of presumably shell companies and concealed cash-out schemes

A law enforcement agency jointly with the SFMS exposed a scheme used to embezzle the funds of state-owned enterprises involved in road construction.

The financial investigation revealed that funds previously transferred by public institutions to enterprises participating in the "Large Construction" state programme as payment for road construction and repairs had been transferred to **Enterprise A** as payment for sand, crushed stone, and soil.

Enterprise A has no mining permits or licenses. It is an intermediary. The enterprise did not actually supply any goods to the enterprises participating in the state program.

Funds received by **Enterprise A** from the enterprises participating in the "Large Construction" programme were subsequently routed through a chain of presumably shell companies as transit transfers paying for various work and services as well as financial aid to business entities that potentially hold cash funds and conduct wholesale and retail business as well as to gambling (lottery) service providers.



Example 3.2.2.

Laundering of proceeds obtained through misappropriation of funds of a community-owned enterprise via affiliated business entities

A law enforcement agency exposed the criminal practices of managers of a community-owned enterprise.

Executives of the community-owned enterprise put in place a scheme for embezzlement of funds intended for renovation of kindergartens and schools in the capital city.

The "scheme" organizers acted through affiliated business entities contracted by them for major repairs and renovations as contractors.

The so-called "partners" completed the work partly and incompletely. Moreover, they did so at heavily inflated prices. Some work had not been completed at all despite having been reported as "finalized".

According to investigation findings, throughout 2019 community-owned enterprises staged competitive bidding on contracts worth more than UAH 100 million, and 30% of this amount was misappropriated and distributed among the scheme participants.

A criminal proceeding has been initiated under Part 3 of Article 191 (misappropriation, embezzlement, or theft of property through abuse of office committed repeatedly or by a group of persons by prior agreement) of the Criminal Code of Ukraine.

Example 3.2.3.

Laundering of proceeds from embezzlement of funds of public institutions

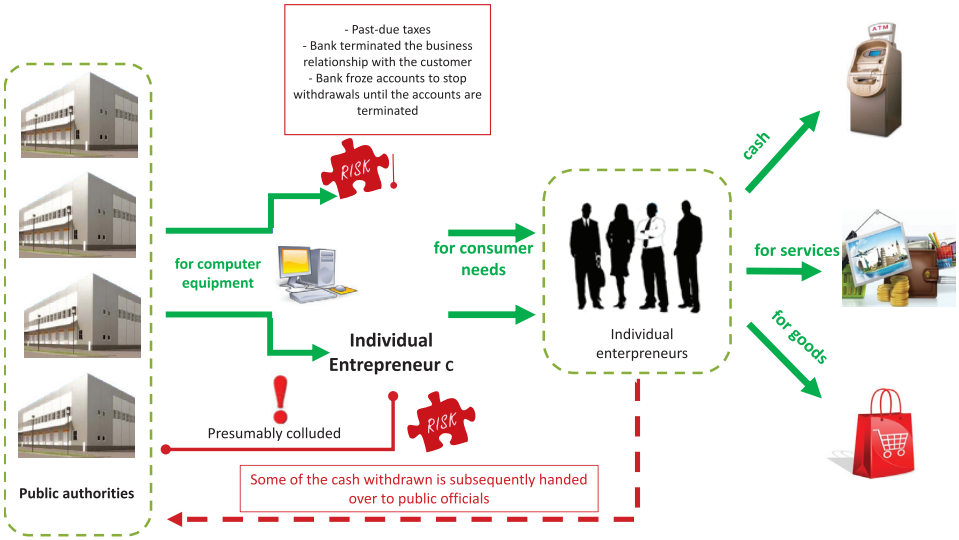
A financial investigation by the SFMS exposed a scheme used to embezzle funds of **Public institutions**.

Specifically, **Public institutions** transferred funds to **Individual Entrepreneur C** who showed signs of fictitiousness (past-due taxes, accounts frozen by the bank and business relations terminated) as payment for computer equipment.

Public funds received by **Individual Entrepreneur C** were transferred to accounts of other **Individual Entrepreneurs** in small installments and transactions. These individuals eventually used the funds for personal needs and withdrew some of them as cash.

Notably, according to the law enforcement agency, officials of the relevant **Public institutions** colluded with the abovementioned individual entrepreneur who later handed over the cash funds to the officials in question.

The law enforcement agency is conducting a pretrial investigation.



Example 3.2.4.

Laundering of proceeds from embezzlement of public funds through shell companies

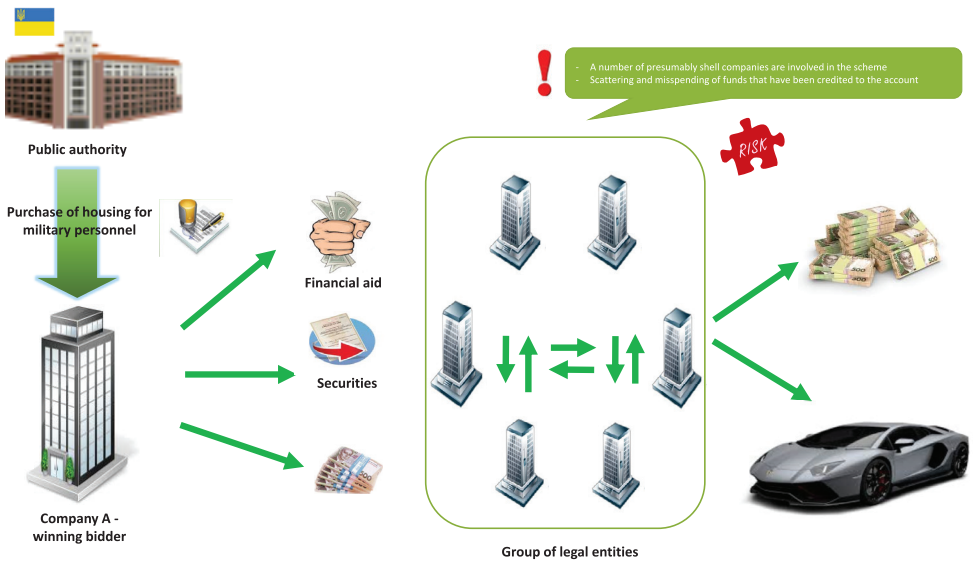
A law enforcement agency jointly with the SFMS exposed a scheme used to embezzle public funds under the guise of procurement of housing for military personnel on co-investment terms, followed by subsequent laundering of these funds.

A financial investigation revealed that a **Public authority** transferred funds to the winning bidder in a tender (**Enterprise A**) as payment for housing for military personnel on co-investment terms.

Enterprise A spent some of the public funds by purchasing securities, extending and recovering financial aid, and withdrawing cash and transferred the remaining funds to accounts belonging to a group of **Legal entities**. The funds were then withdrawn as cash and used to buy an executive-class car.

The **Legal entities** show signs of shell companies: their executive and founder are the same person; they do not pay taxes, have no relevant staff or fixed assets that could be used to perform work and provide services in the scope requested.

The law enforcement agency is conducting a pretrial investigation.



Example 3.2.5.

Laundering of proceeds from embezzlement of public funds through overstatement of the price of the government contract

Based on the law enforcement information, the SFMS exposed a scheme used to embezzle public funds through overstatement of the price of the government contract followed by laundering of illicit proceeds through officials and individual entrepreneurs using the illicit cash-out mechanism.

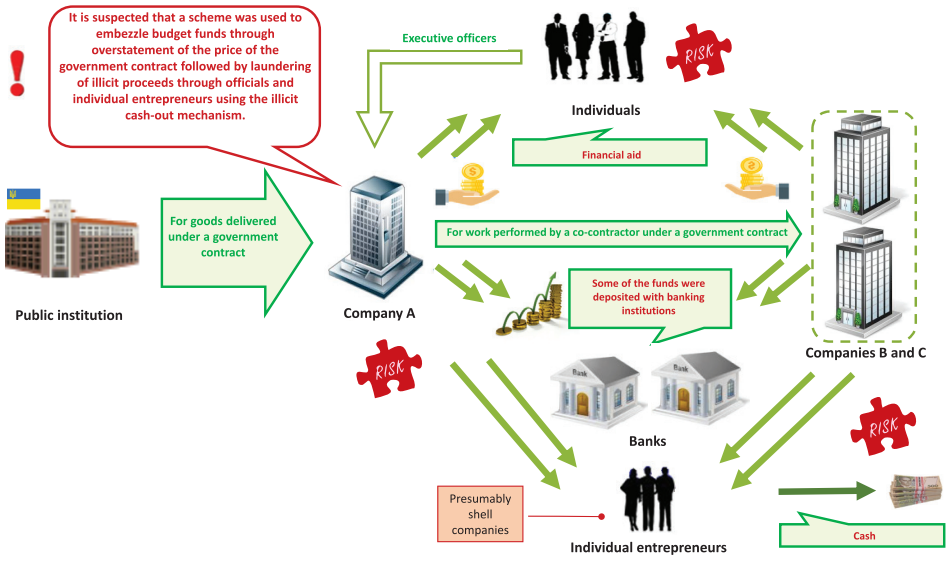
The financial investigation revealed that a **Public institution** transferred public funds allocated for a government contract to **Enterprise A** as payment for manufacture of weapons for the Armed Forces of Ukraine.

Enterprise A engaged **Enterprise B** and **Enterprise C** as co-contractors to manufacture the weapons.

While filling the government order, **Enterprise A** transferred funds received under the government contract to **Enterprise B** and **Enterprise C** as payment for work completed by them.

Enterprise A, **Enterprise B**, and **Enterprise C** misspent the majority of funds. Specifically, they transferred them to their executives as financial aid, deposited them with banking institutions, and transferred them to accounts of business entities showing signs of shell companies (their executive and founder are the same person, they do not pay taxes and do not have employees), which were then withdrawn as cash.

The law enforcement agency is conducting a pretrial investigation.



Example 3.2.6.

Laundering of proceeds obtained through misuse of funds of a community-owned enterprise

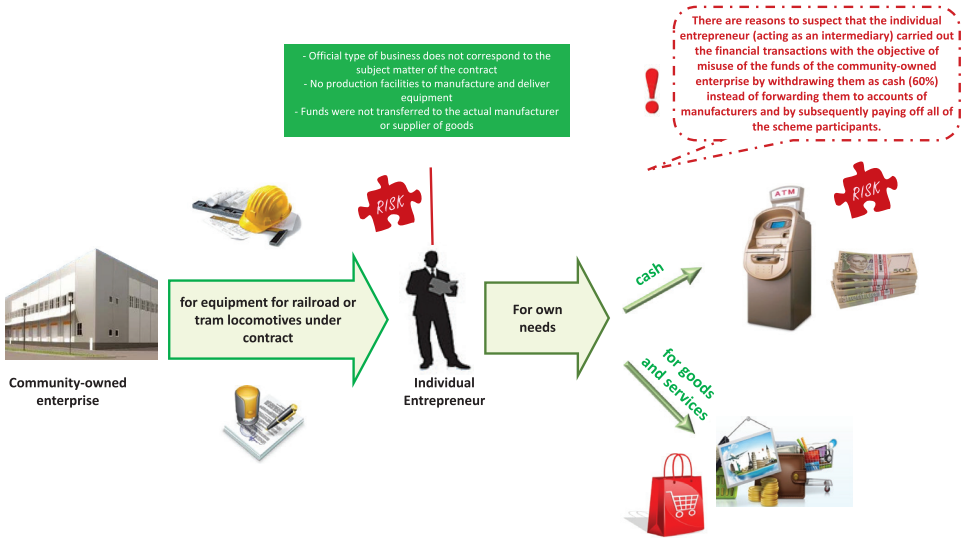
A financial investigation undertaken by the SFMS exposed a scheme of misspending of the funds of a community-owned enterprise paid under a contract for supply of equipment for railroad or tram locomotives to an **Individual Entrepreneur**.

It was established that the community-owned enterprise transferred funds to the **Individual Entrepreneur** as payment for equipment under the contract. The **Individual Entrepreneur** transferred the funds received from the community-owned enterprise to their own accounts and eventually withdrew most of them as cash, while also spending some of the funds on personal purchases.

Notably, the official business of the **Individual Entrepreneur** does not correspond to the subject matter of the contract executed with the **Community-owned enterprise**. The **Individual Entrepreneur** also does not have the production facilities needed to manufacture the equipment. Moreover, the funds had not been transferred to an actual manufacturer or supplier of goods.

In light of this, there is every reason to suspect that the **Individual Entrepreneur** (acting as an intermediary) carried out the financial transactions with the objective of concealing the actual cost of equipment so as to misuse the funds of the community-owned enterprise by withdrawing them as cash (60%) instead of forwarding them to accounts of manufacturers. These transactions were presumably carried out to distribute illicit proceeds among the concerned parties.

The law enforcement agency is conducting a pretrial investigation.



3.3. Laundering of proceeds from tax crimes

The practice of financial investigations demonstrates that demand for unreported cash remains high. Such transactions take place outside the banking system, which significantly complicates detection.

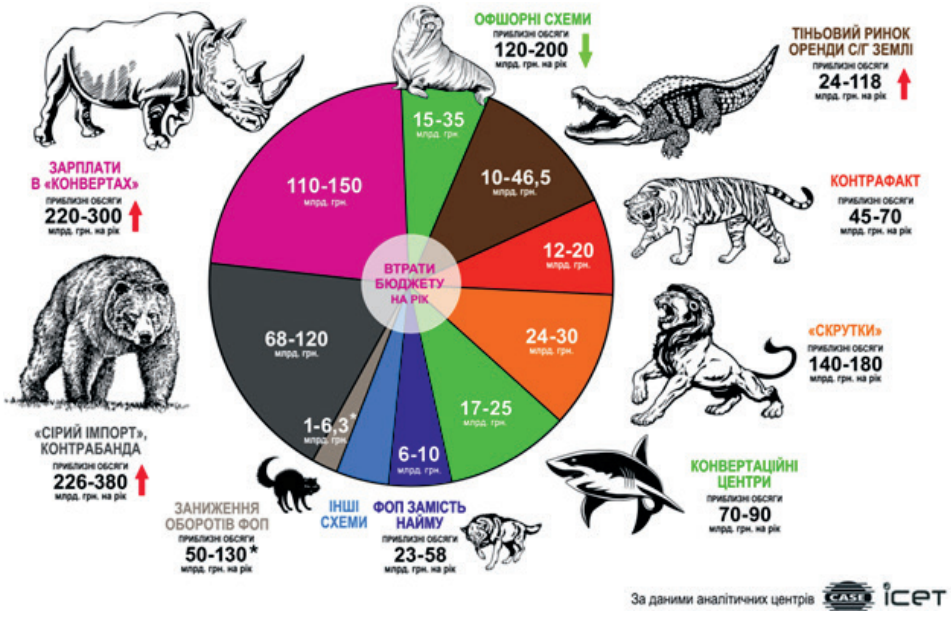
Companies in the real sector of the economy are looking for every opportunity to minimize their value added tax liabilities, hence the high demand for services of "counter cash flows" and fake tax credit.

Tax evasion services are typically provided by professional networks that may consist of legal entities that accumulate funds, transit entities, individual entrepreneurs, and businesses in the real sector of the economy that have cash.

CASE Ukraine and the Institute of Social and Economic Transformation (ISET) conducted a study themed "Comparative Analysis of the Fiscal Effect from the Use of Tax Evasion/Avoidance Instruments in Ukraine: 2021".

https://bit.ly/cxemy_podatky

Comparative analysis of annual volumes of tax evasion and avoidance schemes and their impact on the state budget (2021)



Mechanisms of tax evasion in Ukraine:

- violations of customs regulations and contraband (manipulations with the customs value of goods, "interrupted transit", contraband);
- value added tax theft (illegal refunds from the budget during exports, fictitious entrepreneurship ("missing trader") – in particular "carousel" schemes, substitution of goods ("twists");
- counterfeit goods;
- sheltering income in tax havens (offshore jurisdictions);
- envelope wages;
- distortion of the tax base (concealment of sales volumes);
- abuse of tax rebates, preferences, and special regimes;
- unofficial entrepreneurship and individual business operations without registration.

Common examples relating to money laundering through classical illicit cash-out operations with the use of the "counter cash flows" and "twists" are summarized below.

Example 3.3.1.

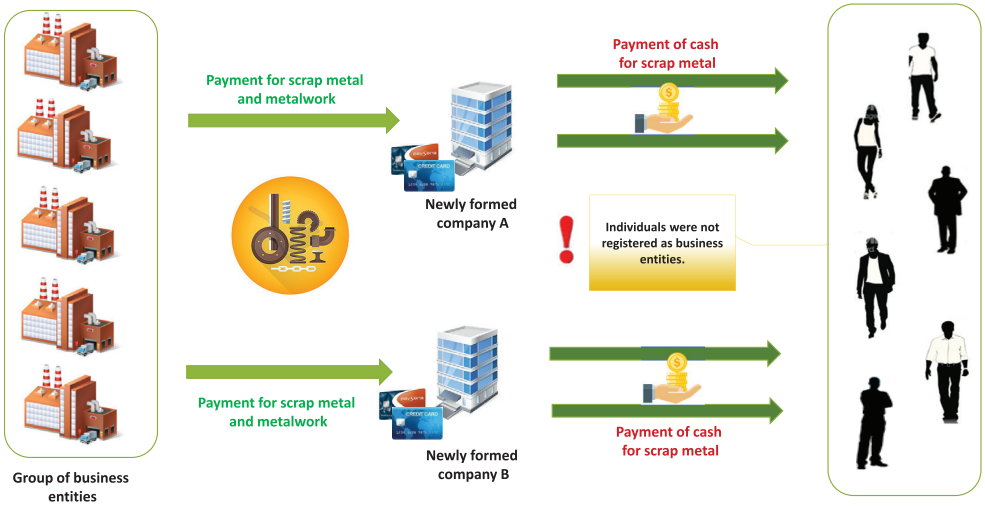
Money laundering with the use of cash through newly formed business entities

Based on the law enforcement information, the SFMS exposed a scheme used to convert non-cash funds into cash through a group of newly formed companies in order to form a tax credit and conceal income.

A financial investigation revealed that looking to form a tax credit a **Group of legal entities** transferred funds to newly formed **Enterprises A** and **B** as payment for metalwork and scrap metal. The funds in question were then converted into cash by a **Group of individuals** under the guise of payment for scrap metal.

These **individuals** were not registered as business entities.

The law enforcement agency is conducting a pretrial investigation.



Example 3.3.2.

Money laundering using "counter cash flows"

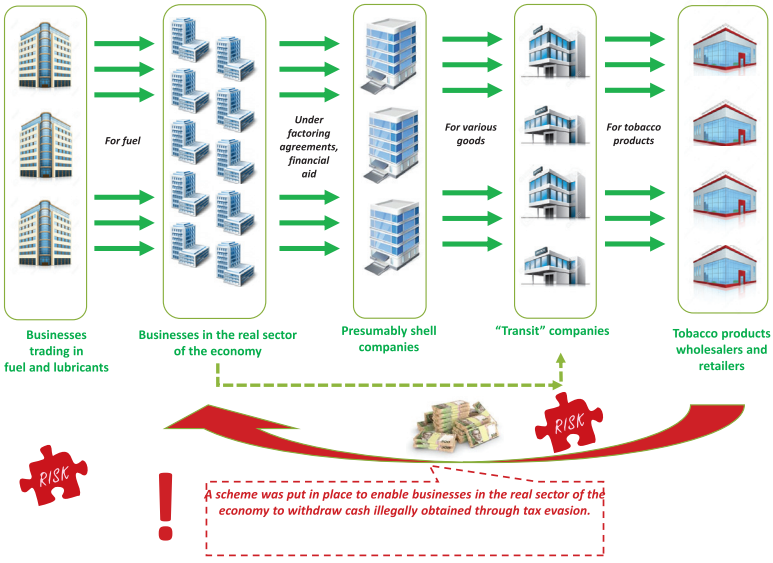
A law enforcement agency jointly with the SFMS exposed a large-scale scheme implemented by a professional money laundering network that helps businesses avoid taxes by artificially forming a VAT credit followed by conversion of non-cash funds into cash using the mechanism of "counter cash flows" through tobacco wholesale and retail businesses.

A financial investigation revealed that a **Group of enterprises** showing signs of shell companies received transfers from a number of **businesses in the real sector of the economy**, which in turn received them from other businesses training in fuel and lubricants.

Notably, funds were transferred to accounts of the **Group of enterprises showing signs of shell companies** (newly formed companies with the same executive and founder, which do not report income or pay taxes, and have no assets required for commercial activity) using such financial instruments as "payment under a factoring agreement" and "financial aid". These instruments are used to break the chain of movement of goods under tax invoices, making it more difficult to link separate business entities into a single cash conversion and transit group.

The investigators tracked down subsequent financial flows from the accounts of the **Group of enterprises showing signs of shell companies**: the funds were transferred through transit companies using the "counter cash flow" mechanism to **Tobacco products wholesalers and retailers**, which provide services involving the conversion of non-cash funds into unreported cash.

The law enforcement agency is conducting a pretrial investigation.



Example 3.3.3.

Laundering of misappropriated funds of banking institutions using the fake tax credit ("twists") mechanism

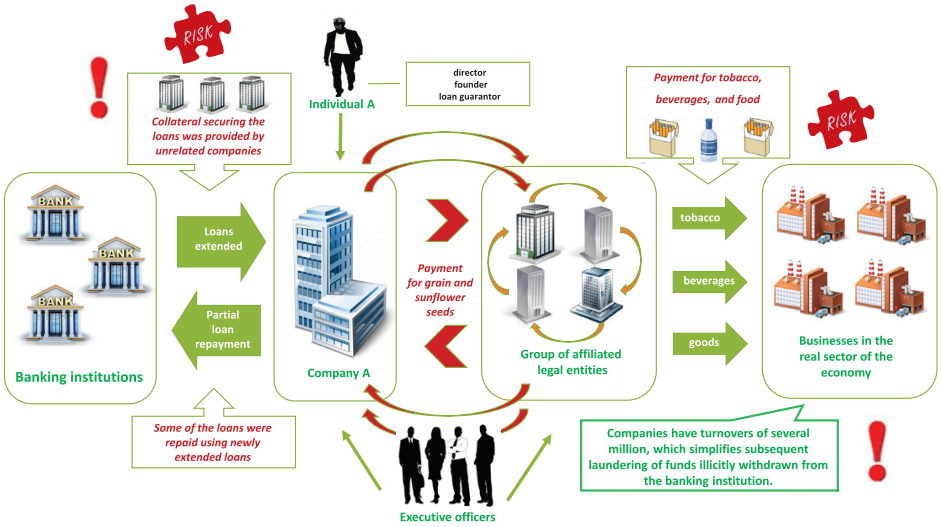
Based on the law enforcement information, the SFMS exposed a scheme used to misappropriate and launder funds of banking institutions using the fake tax credit ("twists") mechanism.

A financial investigation revealed that over the course of one year **Enterprise A** consistently signed loan agreements with various banking institutions while pledging assets of unrelated businesses as collateral. **Individual A** (director and founder of **Enterprise A**) acted as the guarantor.

A portion of funds received by **Enterprise A** under said agreements was then used to repay previous loans (in order to receive the next tranche of the loan). The bulk of funds were transferred to a **Group of affiliated legal entities**. This was followed by a series of cyclical transactions (such as payment for grain crops and sunflower seeds) between the accounts of these legal entities in order to imitate active business operations and improve the image of **Enterprise A**.

At the final stage, these funds were transferred as payment for tobacco, beverages, and food to a **Group of businesses in the real sector of the economy** that have substantial cash turnovers, which simplified the laundering of such funds.

The law enforcement agency is conducting a pretrial investigation.



Apart from schemes involving the laundering of illicit proceeds through classical illicit cash-out centers and with the use of the "counter cash flows" and "twists" mechanisms, there is also demand for schemes involving foreign trade operations.

Such schemes for moving funds abroad are operated by professional networks providing illegal services. These networks typically include Ukrainian legal entities, nonresident companies controlled by Ukrainian citizens, and foreign shell companies that operate for the sole purpose of creating a semblance financial and business operations.

Example 3.3.4.

Money laundering through pseudo imports

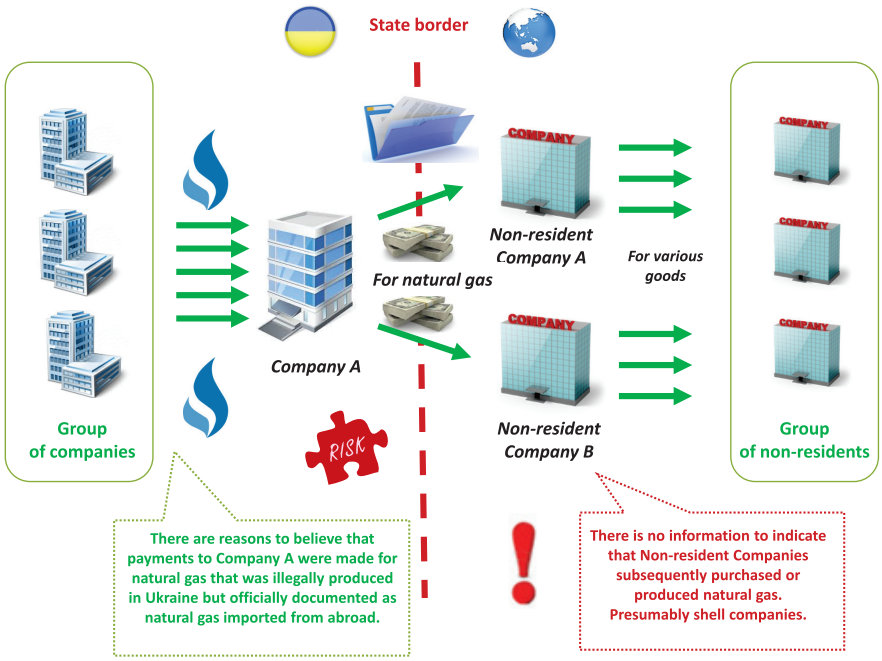
After analyzing information from various sources, the SFMS detected a large-scale money laundering scheme involving proceeds from the sale of natural gas that had been illegally produced in Ukraine.

The financial investigation revealed the following path of financial flows: **Enterprise A** received transfers from a large number of Ukrainian businesses as payment for natural gas. The funds thus accumulated were converted into US dollars and transferred to two **Non-resident Companies** that show signs of shell companies based on data available to the FIU.

The funds were then transferred from the accounts of the **Non-resident Companies** to a large number of other non-resident companies with various details of payment, and only a small portion of those payments were for natural gas.

There is no information to indicate that the **Non-resident Companies** incurred expenses for subsequent procurement or production of natural gas. Therefore, **Enterprise A** paid for natural gas that was illegally produced in Ukraine but officially documented as natural gas imported from abroad.

The law enforcement agency is conducting a pretrial investigation.



Example 3.3.5.

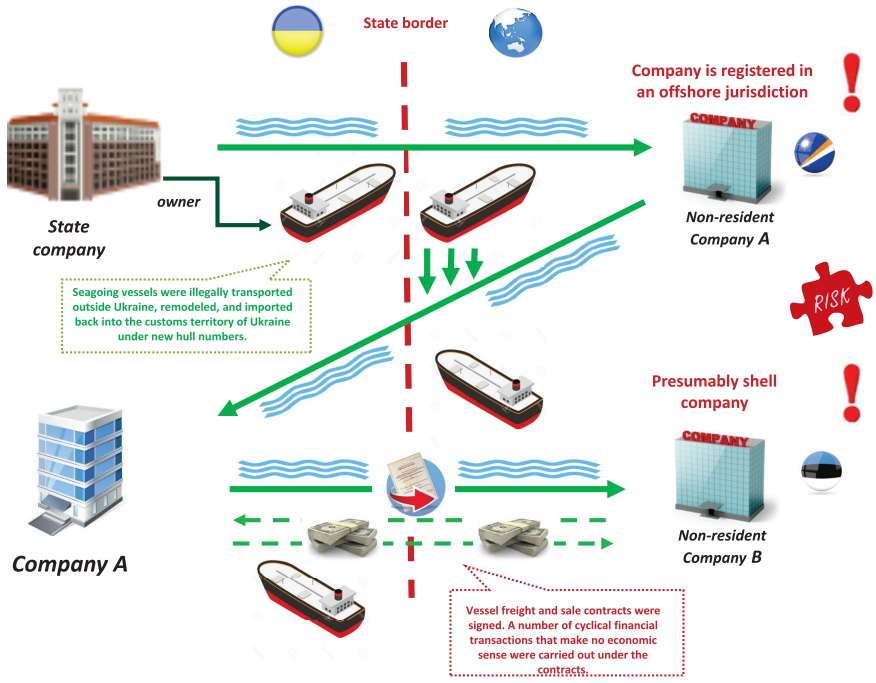
Money laundering through foreign trade operations with the use of presumably fictitious documents

A financial investigation by the SFMS revealed that seagoing vessels owned by a **State company** were illegally transported outside Ukraine, remodeled, and imported back into the customs territory of Ukraine with new hull numbers in favor of **Enterprise A**. The consignor of the vessels was **Non-resident Company A** registered in an offshore jurisdiction.

Enterprise A went on to execute convoluted contracts and agreements that lacked any apparent economic sense with **Non-resident Company B** that shows signs of shell company based on data available to the FIU. The contracts were for freight and subsequent sale of the vessels.

After the funds transferred by **Non-resident Company B** under the contracts were credited to the account, the funds were fully transferred in the opposite direction with various payment details. The purpose of this scheme was to misappropriate state property owned by the **State company** and launder the proceeds of this crime.

The law enforcement agency is conducting a pretrial investigation.



Example 3.3.6.

Money laundering and VAT evasion by applying a discounted rate after issuing the customs cargo declaration

The SFMS detected a tax evasion scheme that involved selling exported grain outside the customs territory of Ukraine without repatriating the foreign currency proceeds from its sale, and money laundering through overseas trade operations.

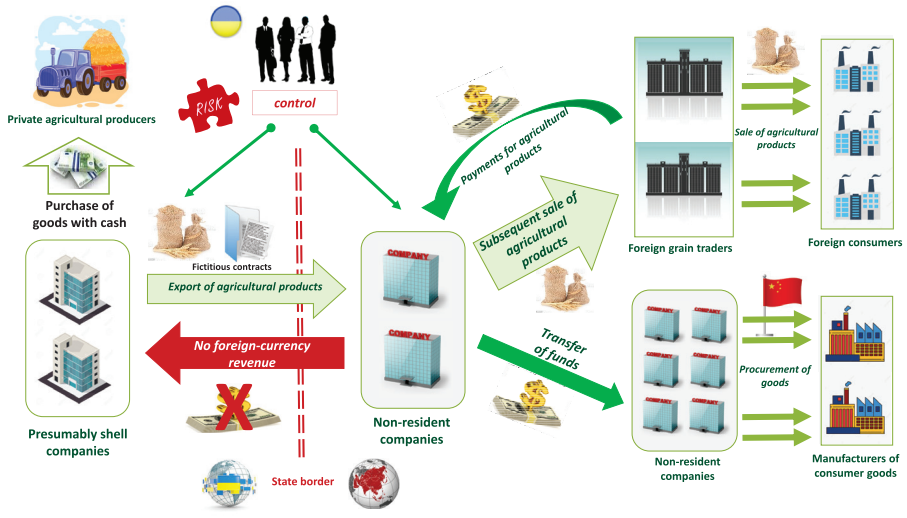
A financial investigation uncovered a professional network providing the relevant illegal services, which consisted of legal entities registered in Ukraine and abroad. As part of this scheme, Ukrainian businesses showing signs of shell companies issued customs cargo declarations under grain export contracts with affiliated **Non-resident Companies**; the grain was procured from individual agricultural producers with cash.

The affiliated **Non-resident Companies** then entered into grain sale contracts with real **Foreign grain traders**. Notably, payments for grain bought between the scheme participants were made exclusively to foreign accounts of the **Non-resident shell companies**. In other words, actual payments for Ukrainian grain exports were made by real buyers outside Ukraine. It was also established that the ultimate beneficial owners of the **Non-resident shell companies** are Ukrainian citizens, some of whom also own the exporting companies.

The funds received by the affiliated nonresident companies from **Foreign grain traders** were rerouted to Asian countries and used to buy consumer goods. The foreign currency export revenue never reached the territory of Ukraine, meaning that the **Ukrainian companies** failed to pay taxes on income generated abroad.

Consumer goods bought overseas and imported into Ukraine (which were paid for using proceeds from the sale of grain) are being sold by wholesalers and retailers that handle large quantities of unreported cash. Some of the cash from the sale of the consumer goods is used in the subsequent cycle to buy another shipment of Ukrainian grain to be exported in another cycle.

The law enforcement agency is conducting a pretrial investigation.



Example 3.3.7.

Money laundering and tax evasion through illegal import operations

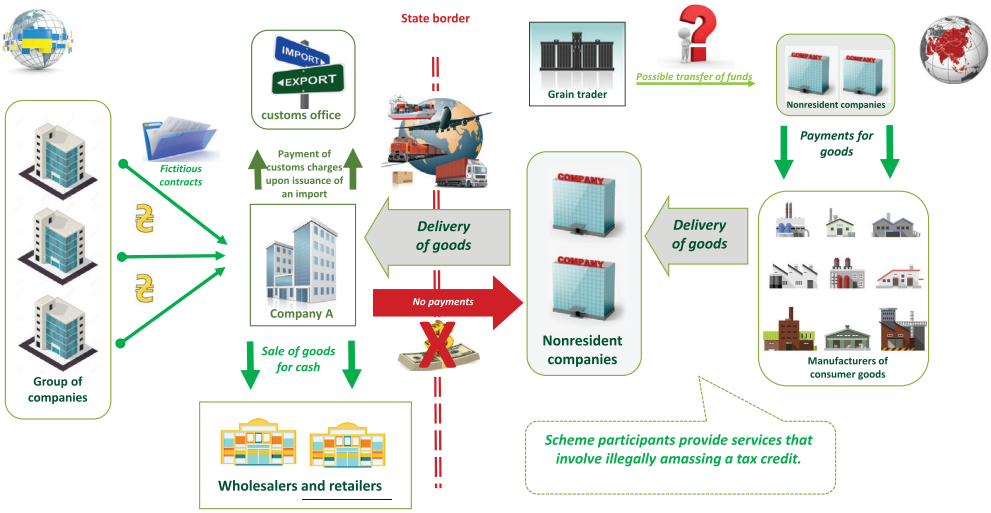
The SFMS detected a scheme used by a professional network providing illegal services.

A financial investigation revealed that **Enterprise A** received funds from a **Group of companies** as payment for various goods. **Enterprise A** transferred the full amount of these funds as payment for customs clearance. Notably, no foreign trade contracts were submitted to the bank, and **Enterprise A** did not transfer funds outside Ukraine.

According to data of the State Customs Service of Ukraine, **Enterprise A** issued import customs cargo declarations for consumer goods received from **Nonresident companies**. These goods were manufactured by various companies most of which are located in Asia. The fact that no payment has been made in favor of the nonresident companies indicates that payments for the imported goods are made outside Ukraine using funds that may have an illicit origin.

The imported goods are then sold through wholesale and retail chains for cash that is not reflected in the books or tax records.

The law enforcement agency is conducting a pretrial investigation.



3.4. Investigation of cases involving terrorism and separatism financing

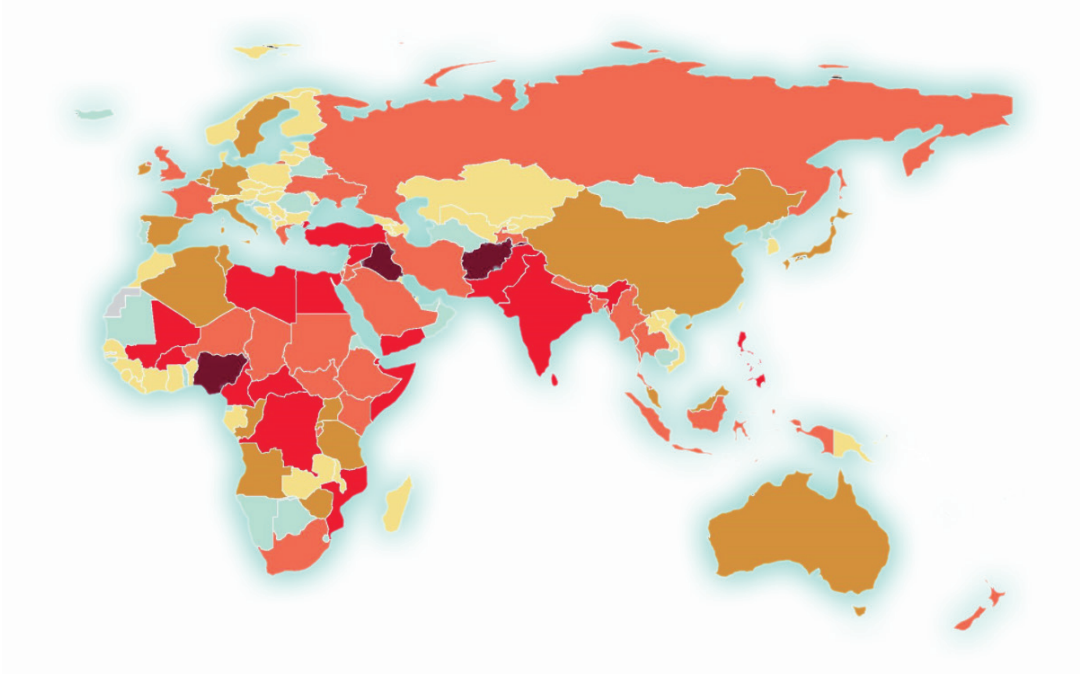
2020 GLOBAL TERRORISM INDEX

The issue of financing of terrorism (separatism) is one of the unresolved problems of contemporary society, which involves a high level of social danger as it may result in human casualties on a mass scale or provoke an armed conflict.

The Global Terrorism Index and the accompanying terrorism threat level ranking of countries has been published annually since 2012.

The Global Terrorism Index is a comprehensive study of terrorist activities all over the world. It reflects the scale of the terrorist threat in a breakdown by country.

The top 10 countries with the highest terrorism threat level for 2020 are Afghanistan, Iraq, Nigeria, Syria, Somali, Yemen, Pakistan, India, the Democratic Republic of Congo, and the Philippines.



RANK	COUNTRY	SCORE	RANK CHANGE
84	Malawi	1.635	↑ 19
85	Denmark	1.484	↑ 15
86	Gabon	1.43	↑ 18
87	Norway	1.297	↑ 40
88	Madagascar	1.19	↓ 7
89	Costa Rica	1.066	↑ 74
90	Argentina	1.024	↓ 8
91	Austria	1.016	↓ 8
92	Kyrgyz Republic	0.95	↓ 8
93	Kazakhstan	0.901	↓ 8
94	Papua New Guinea	0.691	↓ 6
=95	Albania	0.677	↑ 13
=95	Bosnia and Herzegovina	0.677	↓ 9
=97	Benin	0.663	↑ 65
=97	Guatemala	0.663	↓ 8
99	South Korea	0.656	↑ 15
100	Georgia	0.635	↓ 11
101	Taiwan	0.607	↓ 6
102	Morocco	0.565	↓ 11
103	Hungary	0.551	↑ 15
104	Armenia	0.53	↓ 11
105	Guyana	0.477	↑ 26
106	Laos	0.439	↓ 12
=107	Montenegro	0.42	↓ 11
=107	Vietnam	0.42	↓ 11
109	Guinea	0.41	↓ 10
110	Senegal	0.391	↓ 18
111	Czech Republic	0.315	↓ 10
112	Azerbaijan	0.296	↓ 10
113	Switzerland	0.286	↑ 3
114	Poland	0.239	↓ 9
=115	Jamaica	0.229	↓ 11
=115	Lithuania	0.229	↓ 9
=115	Sierra Leone	0.229	↓ 9
118	Liberia	0.191	↑ 7
119	Bulgaria	0.172	↓ 9
120	Trinidad and Tobago	0.162	↑ 15
121	Zambia	0.153	↓ 9
=122	Latvia	0.115	↓ 6
=122	Cyprus	0.115	↓ 8
124	North Macedonia	0.105	↓ 11
125	Uruguay	0.086	↓ 5
=126	Estonia	0.057	↓ 4
=126	Moldova	0.057	↓ 4
=126	Serbia	0.057	↓ 4
129	Lesotho	0.048	↓ 3
130	Djibouti	0.038	↓ 19
131	Slovakia	0.029	↓ 3
132	Panama	0.019	↓ 1
133	Qatar	0.014	⟷
134	Uzbekistan	0.010	↑ 1
=135	Belarus	0.000	⟷
=135	Bhutan	0.000	↓ 27
=135	Botswana	0.000	⟷
=135	Cambodia	0.000	⟷
=135	Croatia	0.000	⟷
=135	Cuba	0.000	⟷
=135	Dominican Republic	0.000	↓ 44
=135	El Salvador	0.000	⟷
=135	Equatorial Guinea	0.000	⟷
=135	Eritrea	0.000	⟷
=135	Guinea-Bissau	0.000	⟷
=135	Iceland	0.000	↓ 30
=135	Kosovo	0.000	⟷
=135	Mauritania	0.000	⟷
=135	Mauritius	0.000	⟷
=135	Mongolia	0.000	⟷
=135	Namibia	0.000	⟷
=135	North Korea	0.000	⟷
=135	Oman	0.000	⟷
=135	Portugal	0.000	⟷
=135	Romania	0.000	⟷
=135	Singapore	0.000	⟷
=135	Slovenia	0.000	⟷
=135	Eswatini	0.000	⟷
=135	The Gambia	0.000	⟷
=135	Timor-Leste	0.000	⟷
=135	Togo	0.000	⟷
=135	Turkmenistan	0.000	⟷
=135	United Arab Emirates	0.000	↓ 34

The risks of the spread of terrorism and separatism in Ukraine currently remain relevant in light of a number of external and internal factors that adversely impact the state of national security.

Factors contributing to the spread of terrorism and separatism in Ukraine

External factors:

growing activity of international terrorist organizations, fomenting of separatist ideas, organizing and financing of activities aimed at compromising the sovereignty and territorial integrity of the country.

Internal factors:

Illicit trafficking of large quantities of weapons and ammo, increasingly more radical public sentiments, etc.

Threats stemming from terrorism (separatism) persist, terrorist groups may attempt to take advantage of the COVID-19 situation in order to step up their activities while governments remain focused on the pandemic.

Traditional practices (methods) of terrorism and separatism financing rely on legitimate sources (proceeds from legitimate business, charitable donations), proceeds of crime (drug trafficking, ransom, fraud), funding from governments that encourage terrorism, as well as funding by terrorists themselves.

Common examples relating terrorism and separatism financing are summarized below.

Example 3.4.1.

Financing of separatism through illegal cryptocurrency exchanges[2]

A law enforcement agency has exposed a network of unofficial cryptocurrency exchanges that permitted anonymous payments and systemic withdrawals of illicit funds and their conversion into cash.

The services of these online exchanges were most commonly used by individuals. Specifically, they were users who received money transfers from e-wallets registered in the aggressor country, which are outlawed in Ukraine.

Among them were organizers of mass protests ahead of Ukraine's Independence Day. They used these exact networks to hire provocateurs.

The network operated since early 2021 and provided money transfer services to over 1,000 customers.

Criminals used this network to transfer close to UAH 30 million on a monthly basis. They would charge a 5-10% commission fee for their services.

The law enforcement agency initiated a criminal proceeding under Article 200 "Illegal activity involving the use of transfer documents, payment cards, and other means of accessing bank accounts, or equipment used to manufacture such means" and Article 209 "Legalization (laundering) of the proceeds of crime" of the Criminal Code of Ukraine.

Example 3.4.2.

Financing of terrorism and separatism through contraband coal shipments

A financial investigation by the SFMS exposed a terrorism financing scheme through payment for coal mined in the temporarily occupied territories of Donetsk and Luhansk Regions. The illicit proceeds were subsequently laundered through importation of illegally mined coal into Ukraine.

Nonresident Company A (a coal importer) received approximately USD 1 million in its account with the payment details stated as "advance payment for coal". The funds arrived from **Enterprise A** (a Ukrainian coal mining company) and were immediately transferred to the account of another **Nonresident Company B** (an intermediary) with a foreign bank that has been accused of facilitating money laundering practices.

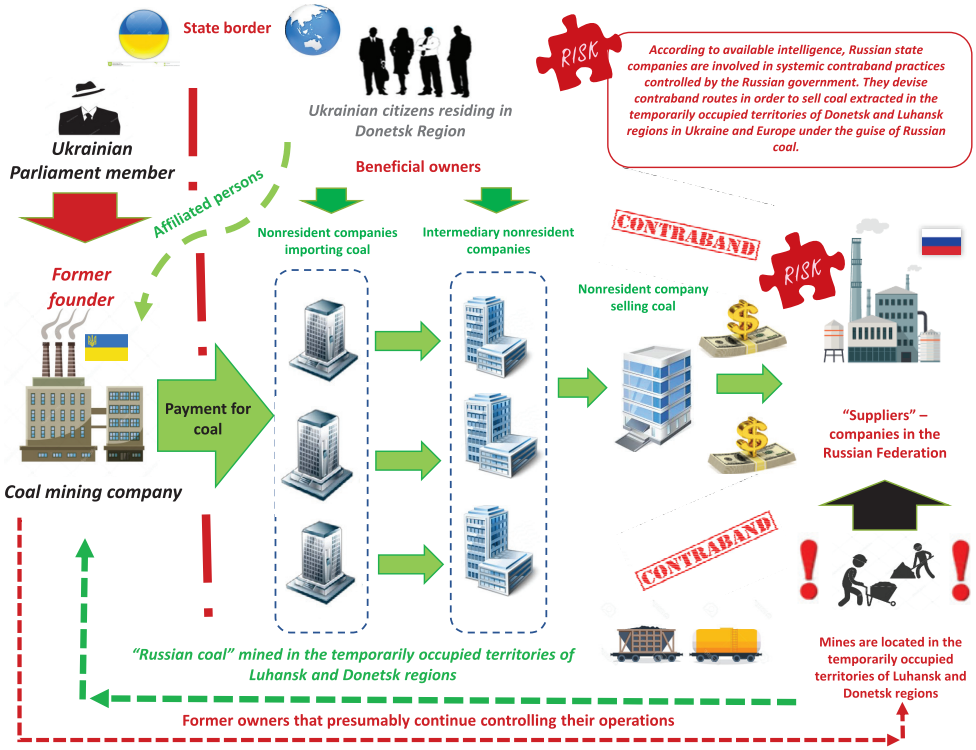
According to the chart of transactions, a nonresident company (an intermediary) bought 20,000 tonnes of coal from a nonresident company (the seller) and then sold it to a nonresident company (a coal importer), which in turn sold it to the ultimate consignee (a Ukrainian coal mining company previously owned by a Ukrainian Member of parliament).

2 Access: https://ssu.gov.ua/novyny/sbu-zablokuvala-pidpilni-kryptoobminnyky-u-kyievi-cherez-nykh-finansuvaly-provokatsii-do-dnia-nezalezhnosti-ukrainy

A review of the contract, customs cargo declarations, and invoices indicated that Russian coal was supposed to be shipped to Ukraine from mines of Kuzbass (Russian Federation). However, other available information and a comparison of the delivery routes demonstrated that such deliveries lacked any economic sense. Freight cars with coal coming from the occupied territories of Donetsk and Luhansk regions were topped up with a small quantity of coal of Russian origin in Rostov region before being sent to Ukraine under the guise of "Russian coal" to avoid detection.

The investigation findings revealed that the beneficial owners of the nonresident companies involved in this scheme are **Ukrainian citizens** — residents of Donetsk Region, who are affiliated with Ukrainian coal mining companies.

The law enforcement agency is conducting a pretrial investigation.



Example 3.4.3.

Financing of terrorism using funds received as a private transfer

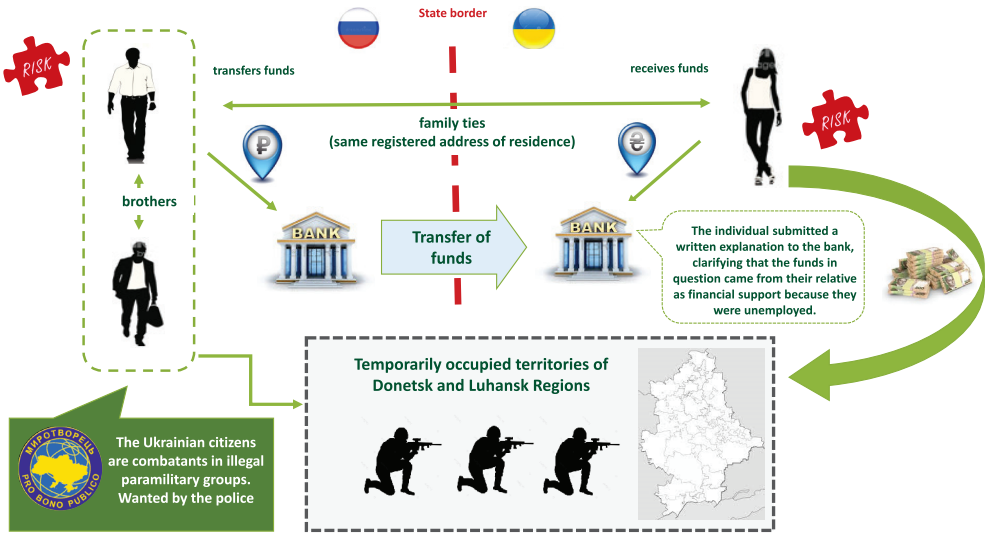
A financial investigation by the SFMS revealed that a large transfer originating in the Russian Federation was credited to the account of an individual registered near the line of separation with the temporarily occupied territories of Donetsk and Luhansk Regions.

The **Individual** submitted a written explanation to the bank, clarifying that the funds in question came from their relative as financial support because of his unemployment.

The financial investigation revealed that the funds originated from a citizen of Ukraine who, along with his brother, are combatants with the illegal paramilitary groups and are wanted by the police. Moreover, these individuals share the same registered address of residence with the recipient of funds.

Funds coming from the Russian Federation from an individual wanted by law enforcement in Ukraine may be intended for recruitment and transportation of volunteers for the illegal paramilitary groups operating in the temporarily occupied territories of Donetsk and Luhansk Regions.

The law enforcement agency is conducting a pretrial investigation.



Example 3.4.4.

Financing of separatism with the use of nonprofit organizations

The SFMS exposed a scheme used by foreign charitable foundations and institutions to fund Ukrainian businesses and nonprofit organizations under the guide of charitable aid and grants: this money was subsequently transferred to accounts of individuals or legal entities.

A financial investigation revealed that in recent years **Charitable foundations and institutions** of a foreign country regularly transferred funds amounting to millions of hryvnias to accounts of **Ukrainian NGOs and businesses** under the guide of charitable aid. The funds in question were subsequently transferred to accounts of IE and legal entities as non-repayable financial aid.

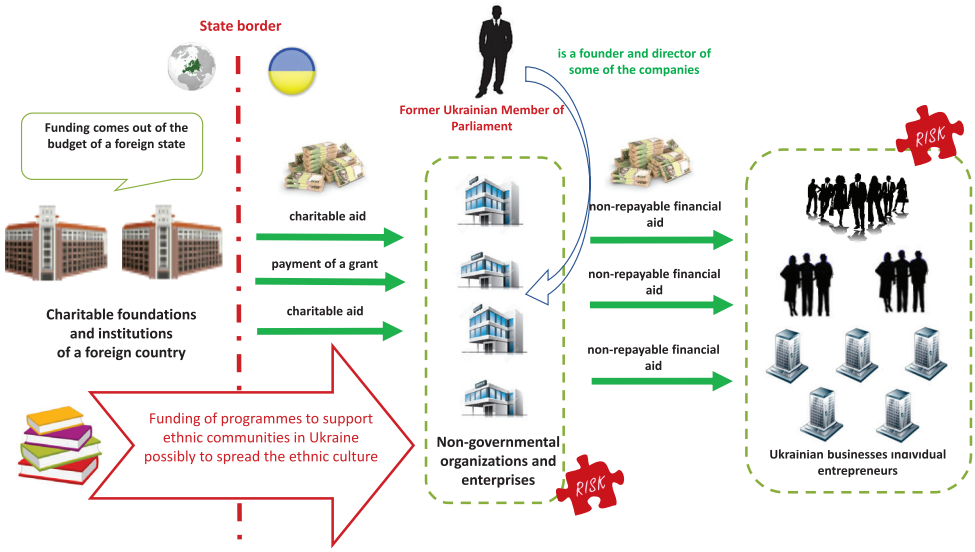
It was discovered that the majority of IE were registered shortly before receiving financial aid.

According to information in the public domain, the government of a foreign country uses **State foundations and institutions** to extend financial aid purportedly meant to facilitate economic growth in the frontier region of Ukraine that borders on this country and has many ethnic representatives of that country in the local community.

Meanwhile, these funds are being used to conceal activities aimed at destabilizing the sociopolitical situation in certain regions of Ukraine by staging anti-Ukrainian radical rallies and activities (distribution of separatist literature, distortion of history, damaging of cultural monuments as a way to incite interethnic strife, and so forth).

A former MP of Ukraine is one of the founders of the companies that received funds from such **foreign NPOs**.

The law enforcement agency is conducting a pretrial investigation.



Example 3.4.5.

Use of non-governmental organizations for the financing of separatism

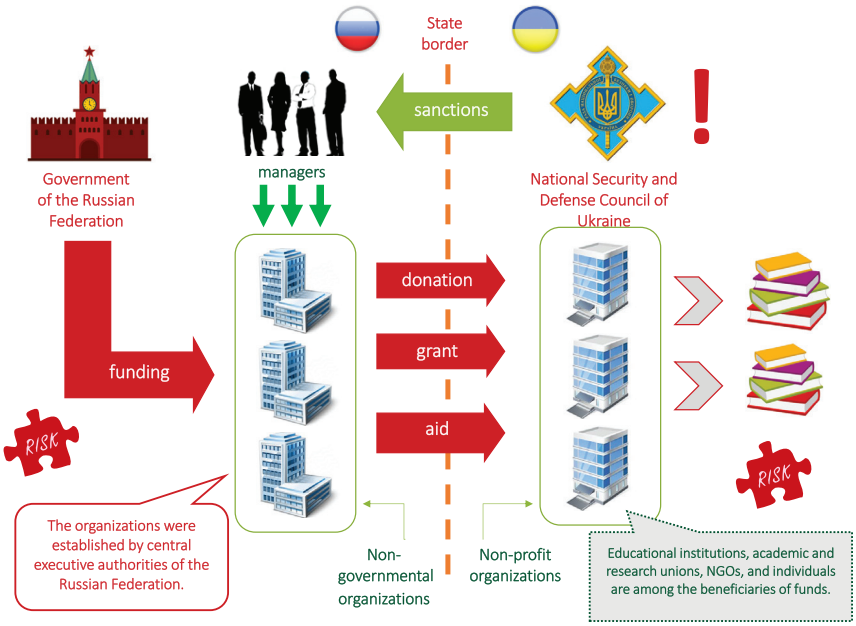
The SFMS has exposed a scheme used by Russian NGOs to fund Ukrainian nonprofit organizations whose goal in Ukrainian territory is to support and popularize Russian standards.

A financial investigation revealed that for a number of years a **Russian NGO** transferred and attempted to transfer funds in the form of grants, aid, or donation to various Ukrainian **Nonprofit organizations** most of which operate in education. The same transfers to these **Nonprofit organizations** arrived from other **NGOs (foundations)** established in the Russian Federation.

It is noteworthy that the founders of these Russian foundations are central executive authorities of the Russian Federation (ministries), while their managers are ranking Russian public officials who have been put on national sanction lists by the National Security and Defense Council of Ukraine.

The **Nonprofit organizations** subsequently transferred the funds to various legal entities and individuals as payment for printing of publications to be distributed at Ukrainian educational institutions and to organize mass-attendance educational events. Notably, the topics of such events give one reason to believe that they are elements of a hybrid war designed to disseminate pro-Russian informational propaganda.

The law enforcement agency is conducting a pretrial investigation.



3.5. Money laundering through the insurance and securities markets

The insurance market is an integral element of the market infrastructure and financial system of any country. An effective insurance market is a crucial component of the market economy and plays a defining role in shaping the economic situation in the country by creating an insurance environment capable of providing insurance coverage for businesses against contingencies, while also providing social support to the population.

Due to its specific nature, the Ukrainian insurance market is extremely vulnerable to getting abused in money laundering schemes.

The following principal criteria can be used to assess the level of risk of transactions carried out with the involvement of insurers:

- collection of an insurance payout by businesses in the real sector of the economy after procuring insurance against perils that are extremely unlikely;
- insurance payout following an artificially created insurance claim;
- payment of agency fees to businesses showing signs of sham companies before they carried out any operations in the market for insurance services that are difficult to verify as having been provided;
- payments made and provisions formed by insurance companies with the use of junk bonds.

For that matter, the financial instrument called junk bonds is oftentimes used in other illegal schemes (moving assets from Ukraine, minimization of tax liabilities, tax evasion, and so forth) that precede money laundering.

Purchase and sale transactions involving domestic government bonds have also become one of the risky tools on the financial market. While this type of securities is rightfully considered one of the most reliable financial instruments owing to their high liquidity and broad applications, the high demand and the specifics of performance of domestic government bond purchase and sale contracts executed on the stock exchange have turned them into a coveted tool used in money laundering schemes, especially for politically exposed persons who are obligated to declare their assets.

Example 3.5.1.

Siphoning of funds through an insurance company and high-risk instruments

The SFMS has exposed a scheme in which a state enterprise entered into sham contracts with an insurance company with the objective of siphoning funds into the shadow economy and subsequently laundering them by purchasing junk bonds, acquiring corporate rights and paying agency fees.

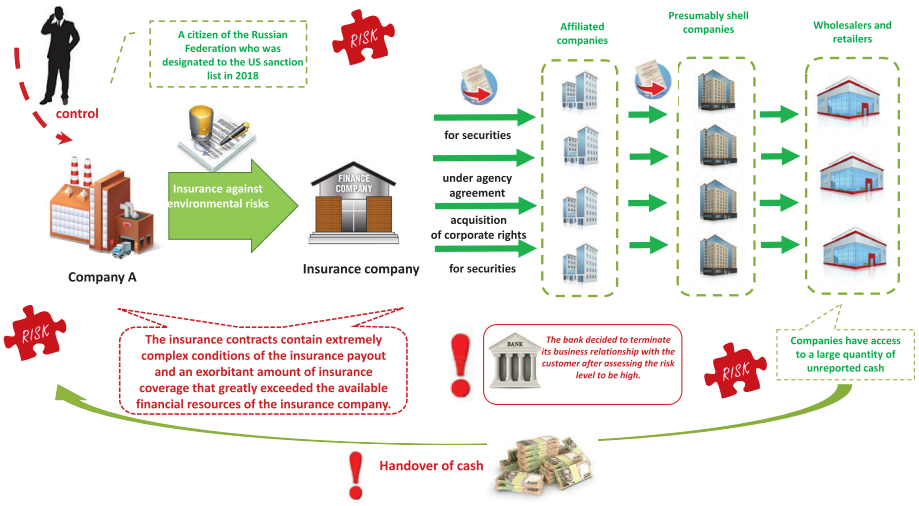
A financial investigation revealed that an **Insurance company** received funds in its bank account as payment of an insurance premium from **Enterprise A** that operated in the nonferrous metals industry. These funds were transferred under environmental risk insurance contracts. The extremely complex conditions of the insurance payout and the exorbitant amount of insurance coverage that greatly exceeded the available financial resources of the insurance company were a red flag pointing to the sham nature of the contract that was not meant to provide actual insurance coverage but had been executed solely for the purpose of siphoning funds out of a running enterprise. It was also established that the operations of **Enterprise A** were controlled by a Russian citizen who was placed on the US sanction list in 2018.

The funds received by the **Insurance company** were subsequently transferred to accounts of affiliated businesses with various payment details: under an agency agreement, under a contract for the purchase and sale of corporate rights, under securities purchase and sale contracts. Meanwhile, the securities purchased belong to the category of junk bonds.

Ultimately, the funds were routed to accounts of businesses showing signs of being sham companies that converted them into cash with the aid of tobacco and alcohol wholesalers and retailers that have large quantities of unreported cash.

Using this scheme, non-cash funds were converted into cash, with insurance-related financial transactions used as a tool for illicit siphoning of funds from a business in the real sector of the economy.

The law enforcement agency is conducting a pretrial investigation.



Example 3.5.2.

Siphoning of funds through an insurance company followed by the use of "counter cash flows"

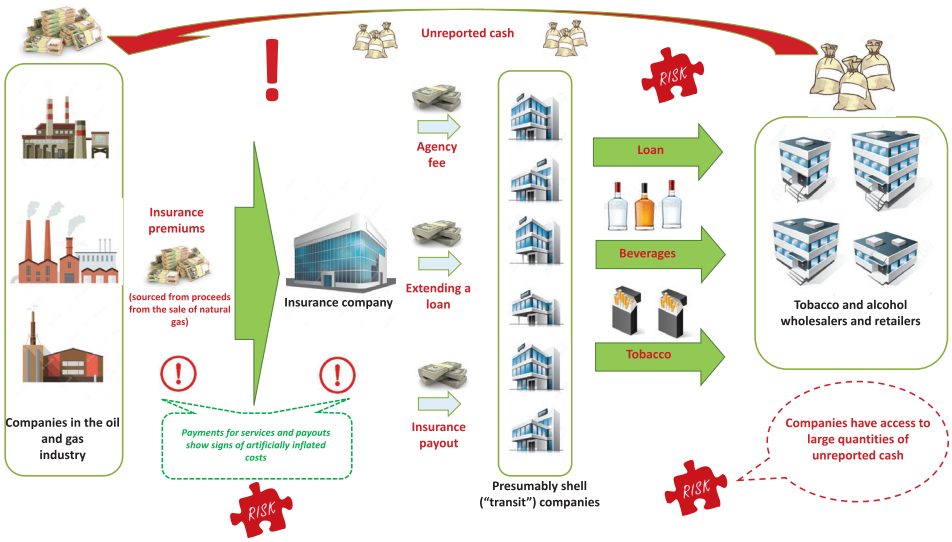
In this scheme, accounts of an insurance company were used to generate tax benefits for businesses in the real sector of the economy and to perform transit routing of non-cash funds with the use of the mechanism of "counter cash flows".

A financial investigation revealed that businesses in the real sector of the economy (including **Oil and gas industry enterprises**) transferred funds to accounts of the **Insurance company** as payment of insurance premiums. The source of funds were proceeds from the sale of natural gas and gas delivery services. Notably, these payments showed signs of an artificially inflated cost of services provided in the oil and gas sector: this led to the generation of super-profits that were subsequently laundered through payments for insurance services.

The funds received by the **Insurance company** were subsequently transferred to accounts of **Transit enterprises** that showed signs of shell companies as payouts of insurance, agency fees, or loans. In turn, these shell companies transferred the funds to **Tobacco and alcohol wholesalers and retailers** as payment under a factoring agreement, loans, or payment for alcohol or tobacco.

Tobacco and alcohol wholesalers and retailers can have large quantities of cash (including unreported cash) that can be used by businesses in the real sector of the economy to exchange their non-cash funds into cash.

The law enforcement agency is conducting a pretrial investigation.



Example 3.5.3.

Falsification of legal transactions to conceal or mask the illegal origin of funds

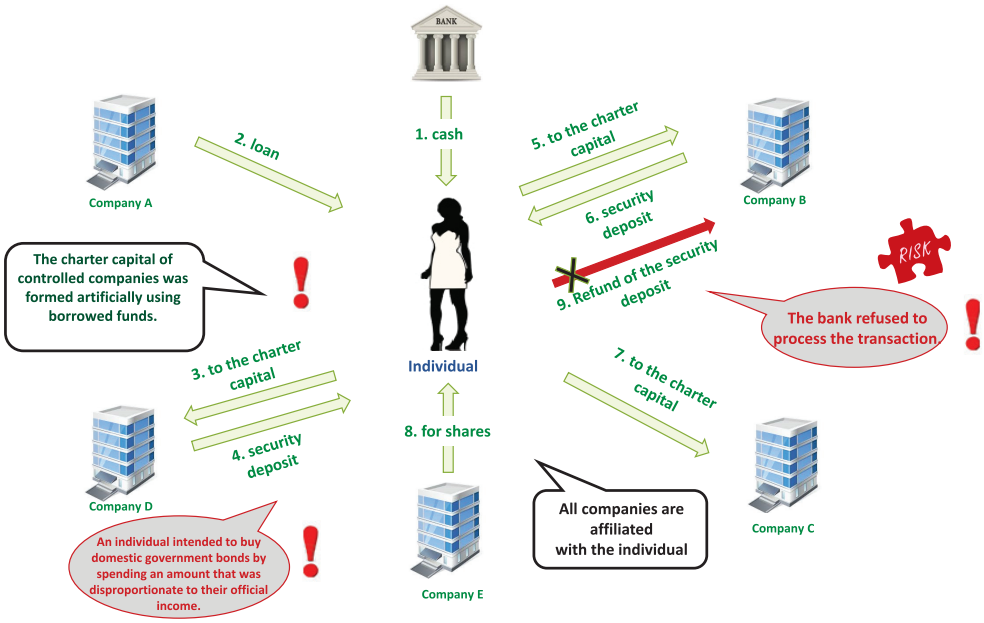
The SFMS exposed a scheme employing the falsification of legal transactions involving the purchase and sale of domestic government bonds with subsequent crediting of the funds to accounts of an individual.

It was established that an **Individual** and companies controlled by them opened accounts with several banking institutions. The individual in question received a loan from **Enterprise A** in one of such accounts, then made a cash deposit and a transfer of funds to the account of **Enterprise B** as a contribution to the charter capital. Enterprise B in turn returned the funds to the individual's account as a security deposit under a contract for the purchase and sale of domestic government bonds. Notably, the **Individual** did not have a sufficient reported income to carry out such transactions. The same scheme was used to carry out major transactions with several other companies at various banks within a short time frame.

The **Individual** then submitted to one of the banking institutions a supplemental agreement terminating the contract for the purchase and sale of domestic government bonds and attempted to return the funds to **Enterprise B**; however, the bank refused to process this transaction. The source of funds for this transaction were proceeds from the sale of shares to **Enterprise D**.

In other words, the **Individual** put in place a scheme that used cyclical financial transactions in order to conceal the illicit origin of funds, which eventually ended up in the accounts of the **Individual**.

The law enforcement agency is conducting a pretrial investigation.



3.6. Laundering of proceeds from arms trade

Law enforcement agencies regularly expose and disrupt criminal activity by individuals involved in trading in arms and highly hazardous chemicals.

The typical masterminds behind such trade schemes are members of criminal groups, individuals with a past criminal record, or other perpetrators with appropriate skill sets.

Below are common examples of investigations into laundering of proceeds from illicit arms trade.

Example 3.6.1.

Money laundering scheme involving proceeds from the sale of weapons and components

Acting on a lead from a banking institution, the SFMS detected financial transactions made using accounts and bank cards of a **group of individuals** allegedly involved in the sale of arms and components originating from the temporarily occupied territories of Donetsk and Luhansk regions.

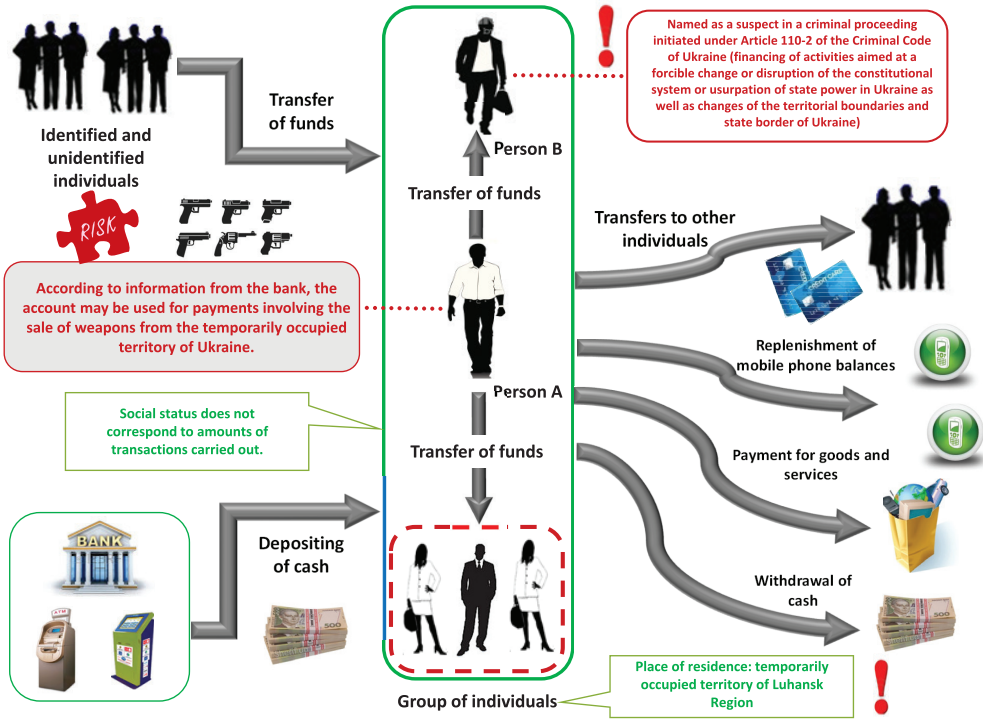
A financial investigation established that the card account of **Individual A** (who was suspected of involvement in the sale of arms originating in the temporarily occupied territory of Ukraine) received non-cash transfers, including with the use of a number of e-money services.

On the same day the funds were transferred to payment cards of a **group of individuals** residing in the temporarily occupied territory of Luhansk region. In particular, the funds were sent to **individual B**, who is named as a suspect in a criminal proceeding involving a suspected crime punishable under Article 110^2 of the Criminal Code of Ukraine: financing of activities aimed at a forcible change or disruption of the constitutional system or usurpation of state power in Ukraine as well as changes of the territorial boundaries and state border of Ukraine.

This **group of individuals** subsequently used the funds to: deposit money into accounts of other individuals, replenish a large number of mobile phone balances, purchase goods or services, and convert funds into cash.

It is noteworthy that there is no information to indicate that the above-mentioned individuals are involved in the operations of any legal entities, are registered as entrepreneurs, have earned or declared any income, or have paid any taxes.

The law enforcement agency is conducting a pre-trial investigation.



3.7. Laundering of proceeds from drug and psychotropic substances trade

The fight against drug crime is one of the most poignant social issues in Ukraine. National Police statistics show that drug crimes account for 16% of all registered crimes.

Notably, every 9th registered serious crime or felony involves trafficking in drugs and psychotropic substances, their equivalents or precursors.

In 10 months of 2021, the National Police documented 272,400 criminal offenses involving drug trafficking, more than 97,000 of which fall in the category of serious crimes or felonies.

The issue of drug trafficking crimes committed by organized groups is as relevant as ever.

Various sources indicate that international drug trafficking is on the rise. A third of all international organized crime rings are involved in drug trafficking.

Latest estimates indicate that transnational organized criminal groups worldwide generate a third of their revenue from drug trafficking.

Organized drug criminal groups are rapidly perfecting their methods and embrace the latest innovative technologies, online communication capabilities, and cryptocurrency transactions, thereby expanding the drug trafficking market.

Drug trafficking as a form of the organized crime also breeds corruption and entangles representatives of the public authorities, including law enforcement officers.

A criminal organisation specializing in drug trafficking stands out for its high level of management and organization. Intermediate structural and functional units have been formed between management and "foot soldiers": advisors, consultants, logistics experts, intelligence personnel, security guards, corrupt public officials, etc.

According to the State Border Guard Service, the quantities of drugs seized at the state border of Ukraine and the risk of their contraband remain high.

Below are common examples of investigations into laundering of proceeds from drug trafficking.

Example 3.7.1.

Detection of international drug and precursor contraband channels

The Security Service of Ukraine has cut off two international contraband channels used to smuggle drugs and precursors into Ukraine. Criminals imported wholesale shipments of their "merchandise" under the guide of medicinal products and cosmetics. On average, the drug traffickers made tens of thousands of US dollars each month.

Law enforcers exposed two drug mules as they were going through customs at the Boryspil International Airport. The criminals tried to smuggle a shipment of pseudo-ephedrine – a precursor used in underground drug labs to make methamphetamine.

In an attempt to conceal their criminal activity, the drug mules claimed to transport medicines in their luggage. After smuggling the "goods" into the country, the criminals planned to sell them through their own network of dealers.

Investigators discovered that the suspects were members of an international criminal group specializing in wholesale drug shipments from one of the African countries.

Another organizer of a drug contraband channel was arrested in Kyiv. Criminals smuggled concentrated cannabis from one of North American countries under the guise of cosmetics.

They used international postal services to ship the "goods".

Law enforcers detained the drug trafficker while he was trying to collect another parcel.

Example 3.7.2.

Detection of international cocaine contraband channels

Law enforcers discovered in the port «Pivdennyi» cocaine smuggled into Ukraine. The shipment was concealed from the customs check.

The drug arrived from the Republic of Ecuador through the container terminal of one of the port operators. It was concealed in structural cavities of refrigerated containers carrying a cargo of bananas. Cocaine was packed in 50 briquettes with a gross weight of almost 60 kg. The seized shipment of cocaine is valued at close to USD 10 million on the black market.

Example 3.7.3.

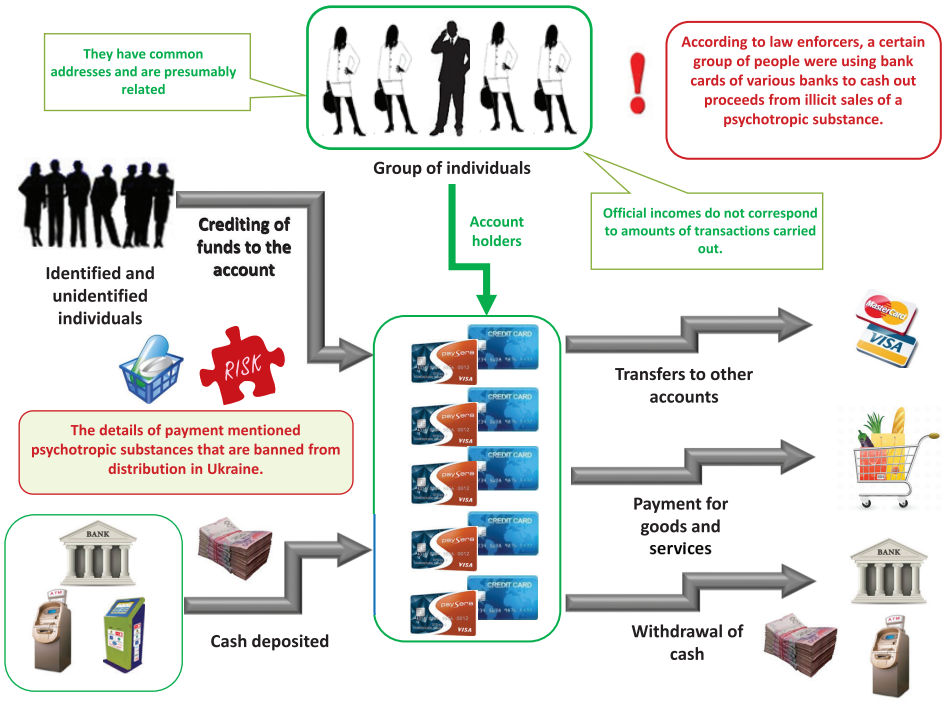
Laundering of proceeds from illicit trafficking in psychotropic substances

The SFMS obtained information from a law enforcement agency about an ongoing pre-trial investigation into a criminal offense punishable under part 2 of Article 307 of the Criminal Code of Ukraine. The pre-trial investigation found that a certain group of people were using bank cards of various banks to cash out proceeds from illicit sales of a psychotropic substance.

An inquiry by the SFMS revealed that accounts of a **group of five individuals** with various banking institutions received cash and non-cash deposits from a large number of identified and unidentified individuals, including as payment for medicinal products. The funds were then transferred to other accounts, withdrawn as cash, or used to pay for goods and services.

The details of payment mentioned psychotropic substances that are banned from distribution in Ukraine. The individuals who were parties to the financial transactions share the same addresses and are probably related. Most of them were not registered as IE. Moreover, the amounts of their financial transactions do not correspond to their officially declared incomes.

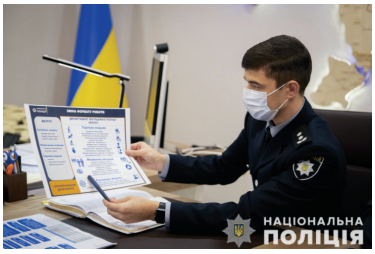
The law enforcement agency is conducting a pre-trial investigation.



3.8. Laundering of proceeds from human trafficking and distribution of pornographic video

Human trafficking and distribution of pornography are a global criminal business, a modern form of slavery that remains one of the most pressing challenges for contemporary legal and economic systems at the national and international levels. There is a need to build capacity of the relevant public authorities in order to combat this type of crime more effectively.

The bulk of these crimes involve labor or sexual exploitation.



Overall, during 7 months of 2021 police officers detected over **760** criminal offenses relating to human trafficking.

Along with these crimes, law enforcers uncovered cases of babies getting sold to buyers abroad.

The police discovered and eliminated **26** organized criminal groups that included **139** members. **328** human traffickers received official notices of suspicion.

Below are common examples of investigations into laundering of proceeds from human trafficking and distribution of pornographic videos.

Example 3.8.1.

Sale of babies to buyers abroad

According to the Migration Policy Department, the organized criminal group consisted of five individuals who sold babies to buyers abroad under the guise of surrogate motherhood.

The criminals formed a **Limited liability company** to provide intermediation services as part of a surrogate motherhood programme.

They published ads for their services on Internet platforms of various countries. The criminals used a tried-and-true scheme: they would find women who agreed to enter into a fictitious marriage with foreigners for a monetary reward of **USD 300 to 1,000**.

One member of the organized criminal group was a doctor who issued fake medical opinions on contraindications that so-called "wives" had against conceiving a child and giving birth. This justified the application of auxiliary reproductive technologies.

In due course, the group would find surrogate mothers for such "married couples".

Women were paid **USD 6,000 to 8,000** for bearing a child.

After giving birth, the mother would grant a power of attorney authorizing the foreign parent to take the child abroad. Foreign citizens paid close to **USD 70,000** for the services of these criminals.

So far the police established 16 instances in which children were sold. Officers seized personal records during searches. They contain information about **160** more orders from foreigners.

Example 3.8.2.

Fictitious employment

According to the National Police of Ukraine, the criminal organization consisted of five individuals who defrauded **192** people out of half a million hryvnias.

The organizers of the criminal scheme established several legal entities to provide intermediation services involving employment abroad. A pretrial investigation by the police revealed that the companies were not licensed to provide such services.

The suspects received a notice of suspicion of having committed a crime punishable under part 4 of Article 190 "Fraud" of the Criminal Code of Ukraine.

Example 3.8.3.

Distribution of pornographic videos

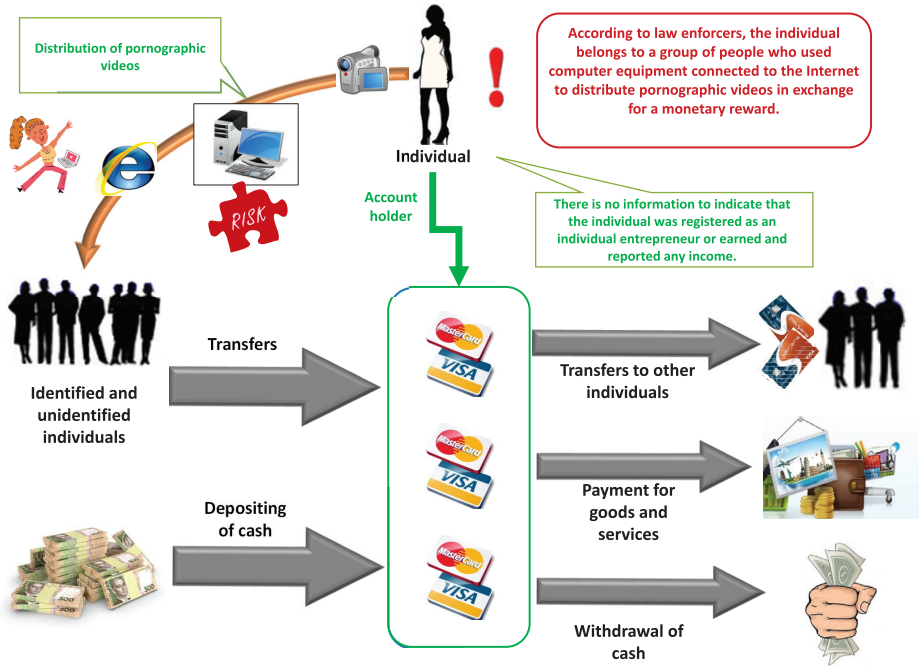
The SFMS obtained information from a law enforcement agency about an ongoing pre-trial investigation into a criminal offense punishable under part 3 of Article 301 and part 2 of Article 209 of the Criminal Code of Ukraine. A pre-trial investigation identified a group of individuals who used computer equipment connected to the Internet to distribute pornographic videos in exchange for a monetary reward.

The SFMS discovered that non-cash and cash payments from a large number of identified and unidentified people were credited to card accounts of an **individual**.

This **individual** then used these funds to purchase goods and services, replenish balances of other individuals, or withdraw them as cash. The majority of cash deposit and withdrawal transactions were performed by the **individual** who owned the card accounts.

This **individual** is not an executive or founder of business companies. There is no information to indicate that the individual was registered as the IE or earned and reported any income.

The law enforcement agency is conducting a pre-trial investigation.



3.9. Laundering of proceeds from fraud

According to the SFMS data and information in the public domain, criminals are attempting to benefit from the COVID-19 pandemic by stepping up their fraudulent activities.

According to data of the Prosecutor General's Office, fraud accounts for a substantial share of all crimes. And yet considering the high latency of this crime (especially unreported fraud), there is reason to believe that this percentage is much higher.

The problem of fraud remains a pressing issue for decades now.

According to applicable provisions of the Criminal Code of Ukraine, fraud can be interpreted from three perspectives: in the narrow sense (fraud proper), in the broad sense, and in the broadest possible sense. More specifically:

- fraud in the narrow sense (fraud proper) implies misappropriation of the property of another person or acquisition of title to property through deceit or abuse of trust, which is punishable under Article 190 "Fraud" of the Criminal Code of Ukraine;
- fraud in the broad sense also includes misappropriation of special-purpose property and other items designed for specific applications, in particular:

  Article 262 "Theft, misappropriation, extortion involving firearms, ammo, explosives or radioactive materials, or misappropriation of the latter through fraud or abuse of office" of the Criminal Code of Ukraine;

  Article 289 "Illegal entry into possession of a vehicle" of the Criminal Code of Ukraine;

  Article 308 "Theft, misappropriation, extortion involving narcotic substances, psychotropic substances or their equivalents, or misappropriation of the latter through fraud or abuse of office" of the Criminal Code of Ukraine;

  Article 312 "Theft, misappropriation, extortion involving precursors, or misappropriation of the latter through fraud or abuse of office" of the Criminal Code of Ukraine;

  Article 313 "Theft, misappropriation, extortion involving equipment designed for manufacture of narcotic substances, psychotropic substances or their equivalents, or misappropriation of the latter through fraud or abuse of office and other illegal acts with the use of such equipment" of the Criminal Code of Ukraine;

  Article 357 "Theft, misappropriation, extortion involving documents, stamps, seals, or misappropriation of the latter through fraud or abuse of office or damage caused thereto" of the Criminal Code of Ukraine;

  Article 410 "Theft, misappropriation, extortion by a military service person involving weapons, ammo, explosives or other items intended for armed combat, vehicles, military or special-purpose hardware or other military property, or misappropriation of the latter through fraud or abuse of office" of the Criminal Code of Ukraine;
- fraud in the broadest sense also includes fraud involving financial resources, which is punishable under Article 222 "Financial fraud" of the Criminal Code of Ukraine.

Below are common examples of investigations into laundering of proceeds from fraud.

3.9.1. Fraud committed with the use of an automated teller machine (ATM), networks of payment terminals, remote service systems, and social engineering

Owing to the variety of instruments for providing services, the financial sector is an appealing target for the application of fraudulent schemes.

This is a constant problem, and the only variable is the number of fraud cases involving specific instruments.

The principal factors behind the transformation of modern fraud practices are the transition of the global economy to a new technological paradigm, informatization of society in all areas, and globalization.

However, such social phenomena as fraud are also finding their way into the virtual world along with these new real-world capabilities.

To sum up, the following types of fraud are known to exist:

Fraud committed with the use of an automated teller machine (ATM):

- cash withdrawal using fake (white plastic) cards;
- use of skimmers (copying of payment card data, including from the magnetic tape, stealing the PIN, etc);
- cash withdrawal in an ATM without reflecting this transaction in the account (Transaction Reversal Fraud);
- cash withdrawal by a bank card owner without obtaining a physical card (Cash Trapping);
- physical attacks on ATMs.

Fraud targeting the network of payment terminals:

- transactions performed using a fake, stolen, or lost bank card;
- cash withdrawal at the bank using fake IDs and a fake bank card;
- duplicate transactions performed by the cashier or operator;
- unauthorized or inaccurate debiting (the amount in the receipt and the purchase amount differ);
- cashiers stealing payment card details while serving customers in order to subsequently make unauthorized use of such details;
- use of skimmers on terminals that steal payment card details during payment processing (criminals conspire with cashiers);
- installation of malware that compromises the software of terminals.

Fraud in remote service systems:

- unauthorized tampering and/or installation of malware (viruses) that compromise computer software and intercept account passwords, secret key or token data, etc.

Social engineering:

- scammers gain the trust of account or card holders to fool them into disclosing their personal data, payment card details, or into transferring funds to accounts of scammers.

3.9.2. Use of digital technologies to commit fraud

The digital economy has been growing rapidly in Ukraine in recent years.

The spread of online services and the transition to electronic interaction between society and the government represent a logical consequence of technological progress.

During the COVID-19 pandemic, many people use online banking, receive account statements on their mobile phones, and order goods or services on the Internet.

This attracts the attention of criminals who seek access to the victim's services in order to commit fraud. A mobile phone number is one of the most critical elements needed to gain or restore access to various devices and electronic services.

According to the Committee on Digital Transformation of the Verkhovna Rada of Ukraine, the majority of mobile subscribers in Ukraine use mobile connection services anonymously, meaning that this problem is acquiring a nationwide dimension.

In reality, most mobile numbers are already linked to specific individuals through banking services.

Official registration of mobile numbers with providers of electronic communication services helps protect users against fraudulent schemes.

There have been multiple cases where unfortunate misunderstandings with banking institutions occurred when customers had their mobile phones with personal data stolen. Criminals also abuse the gullibility of victims to gain access to bank card details, CVV numbers and PINs.



Example 3.9.2.1.

Fraud committed using stolen SIM cards

After establishing control over the phone number, the fraudster gains access to the victim's online banking account and is therefore able to manage the victim's funds.

This is a standard algorithm used by criminals to establish control over the financial number.

Step 1: Forming the log of the latest calls. The criminal calls the victims from different phone numbers in the hopes that you will call back. In this way the criminal is forming a log of incoming and outcoming calls.

Step 2: Balance top-up amount. The fraudster simultaneously deposits a small amount to your mobile phone balance.

Step 3: Contacting the operator. Armed with information collected at the first two steps, the criminal contacts the mobile operator to have the SIM card reissued. Information about the most recent calls and the top-up amount is often enough for the operator to reissue the SIM card.

Step 4: Accessing your online banking profile. Now that the criminal has control over your phone number, they can log into your personal online banking account. The criminal will also receive all SMS notifications with confirmation codes that the bank sends out when processing transactions, granting access to mobile apps, etc.

Example 3.9.2.2.

Hijacking the customer's profile with a mobile operator

Fraudsters attempt to hack the victim's customer profile in the mobile operator's app in order to configure forwarding to a phone number controlled by them.

This is a standard algorithm used by criminals to establish control over the financial number.

Step 1: Fraudsters use the victim's phone number to try and reset the access password for the customer profile. The SMS message with the new access code for the customer profile or the password reset code is sent to the victim's phone number.

Step 2: The criminals call the victim and try to talk them into disclosing the code received from the mobile operator. Knowing that the victim is the customer of the specific mobile operator, the fraudsters can use various social engineering techniques, impersonate an employee of the bank or mobile operator, etc.

Step 3: The fraudsters modify the settings of the customer profile: they set up forwarding to a controlled phone number, change passwords, and take other steps needed to make the crime happen.

3.9.3. Credit fraud

According to law enforcement reports, there is a growing number of cases where criminals take out loans by impersonating others.

The police uncovered mass-scale operations where citizens were subjected to extortion over online loans that criminals took out on their behalf.

Participants of this scheme administered databases of so-called "clients" and maintained records of pseudo debts. Criminals use special-purpose software for anonymization of phone numbers during calls where they threaten the victims.

Example 3.9.3.1.

Online loans taken out on behalf of other people

According to the National Police of Ukraine, an **Individual** used social engineering techniques to take out online loans on behalf of other people with various financial and microlending institutions.

The **Individual** used comprehensive social engineering to gain illegal access to the financial mobile number, email and social media accounts of citizens.

The criminal scanned the compromised accounts to find the identity information needed to take out online loans, specifically passport data and other details.

The criminal then faked passport data and replaced the victim's financial mobile number with her own in order to gain access to the victim's online banking profile. This enabled her to not only withdraw loans but also take out other loans on behalf of the victims.

Investigators also found that in one case the criminal guessed the password to a victim's email account that stored copies of documents and personal photos. The criminal then used this information to access the victim's online banking profile. She then impersonated the victim (as a client of the bank) and initiated data transmission through BankID to access the Diia app on the victim's device.

The Individual received a notice of suspicion of having committed a crime punishable under part 3 of Article 190 "Fraud" of the Criminal Code of Ukraine.

3.9.4. Fraud committed through identity theft

Data thieves usually gain access to personal data (information) of the victim (passwords, passport details, credit card data, etc.) and use them for their own needs by impersonating the victim.

Stolen confidential information (for instance, from Facebook, Viber, or WhatsApp) can be used for various illegal purposes. Thieves can also copy or hijack a person's social media profile or steal a victim's mobile phone number and then contact the victim's friends.

Example 3.9.4.1.

Social network identity theft

An **Individual** stole another person's identity on Facebook and used Facebook Messenger to contact the person's friends on the social network asking them to lend money for some urgent expenses.

Once the friends agreed to lend money, the **Fraudster** gave them bank card details for the money transfer.

3.9.5. Fraud involving lotteries, prizes, and winnings

The fraud scheme involving lotteries, prizes, or winnings typically begins with the potential victim receiving an email, phone call, or text message about having won a large amount of money, a valuable prize, etc.

The user is usually informed that the time to collect the winnings is limited and that they need to pay tax, delivery costs, or cover other imaginary expenses.

Since such communications about lotteries, prizes, or winnings are a scam, the victim never receives the anticipated "prizes" after paying the criminals.

Example 3.9.5.1.

Fraud under the guise of a reward for taking a public opinion poll

According to the National Police of Ukraine, criminals use various social networks to spread a video where a Ukrainian TV presenter talks about rewards for completing a consumer market public opinion poll.

The fraudsters provide a video description with a link to a site where the poll can be allegedly completed and the monetary reward collected.

The criminals also post fake comments about successful receipt of the reward.

After completing the pseudo poll, users are invited to enter bank card details to pay a "commission fee" and receive the reward. However, by following through with this the users not only transfer funds to fraudsters but also disclose their banking details which the scammers can use as they please.

3.9.6. Fraud committed by impersonating an official

One way in which criminals commit fraud involves impersonating representatives of the public authorities or banking institutions.

The criminals contact potential victims (in person, by email, by phone or text message) and impersonate officials of various institutions or organizations in order to gain access to personal banking data or cash.

In some cases criminals impersonate representatives of law enforcement, hospitals, or banking institutions.

They mislead victims into thinking that something bad happened with their relatives who need urgent assistance or face criminal prosecution, or that their bank card has been blocked.

Also, in order to commit a "blocked card" scam criminals impersonate employees of a banking institution in order to obtain confidential financial information from victims.

Example 3.9.6.1.

Fraud involving a "blocked card" scam

According to the Cyberpolice Department of the National Police of Ukraine, an **Individual** impersonated a bank employee and sent out messages to citizens to the effect that their bank cards have been blocked.

The message included a phone number that the victim had to call and discuss how to "unblock" the card. The **Individual** persuaded the victims to disclose the complete card details. After gaining access to the card data, the criminal stole the victims' funds.

The police initiated a criminal proceeding under part 3 of Article 190 "Fraud" of the Criminal Code of Ukraine.

Example 3.9.6.2.

Fraudulent appropriation of funds of legal entities with the use of forged documents

The SFMS discovered that unidentified individuals used the bank account of a private court enforcement officer in order to fraudulently misappropriate the funds of a number of legal entities in the pharmaceuticals industry located in various cities of Ukraine by sending debt recovery claims to Ukrainian banking institutions.

It was established that attempts were made to debit funds from accounts of **three pharmaceutical companies** with two banking institutions and transfer them to the account of the **private court enforcement officer** with another banking institution under the guise of debt recovery pursuant to court enforcement orders. The banking institution suspended the financial transactions.

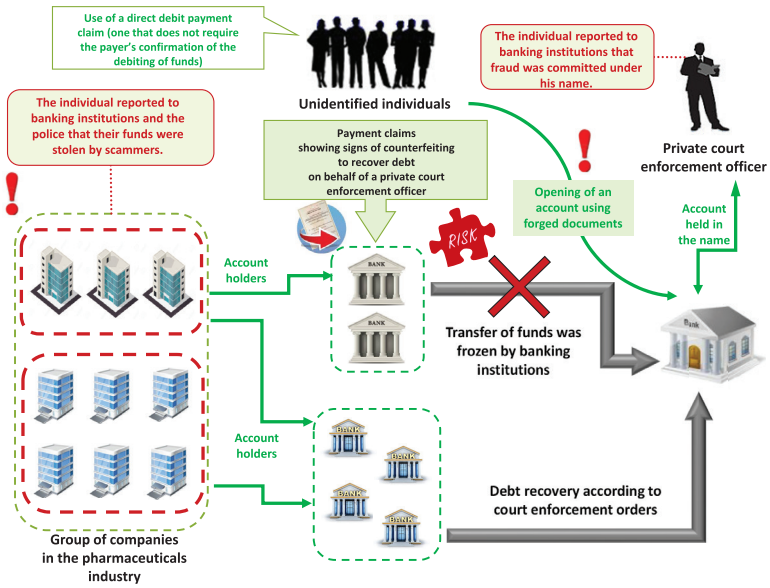
Attempts to debit the funds were made using direct debit claims (they permit transferring funds to the beneficiary's account without having to obtain the payer's approval).

The companies contacted the banking institution and the police to report fraud committed by unidentified individuals impersonating a **private court enforcement officer**. The real **private court enforcement officer** made it known that he did not open the account in question and did not send out the payment claims.

A review of documents presented by various banking institutions revealed that the signatures of the **private court enforcement officer** were different, which proved that document forgery occurred.

It was also established that the account opened on behalf of the private court enforcement officer received transfers from another group of pharmaceutical companies with the same payment details and during the same period.

The law enforcement agency is conducting a pre-trial investigation.



3.9.7. Online shopping fraud

One of the most common online fraud schemes involves scamming of online shoppers.

The number of such cases has increased during the pandemic, particularly due to a shortage of certain categories of goods.

Criminals create fake sites posing as a reputed seller in order to sell expensive branded products at extremely low prices.

However, after placing the order the buyer would receive a fake product or nothing at all. As a worst-case scenario, the criminals could steal all assets using the victim's personal data (bank card details).

It is advisable to find out more about the seller in order to minimize the risk of financial losses due to this type of fraud.

Example 3.9.7.1.

Money theft though phishing online stores[3]

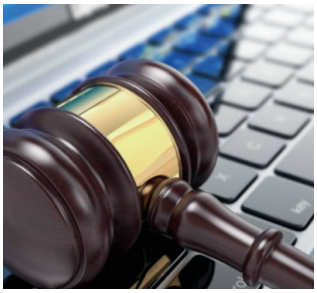
According to the Cyberpolice Department of the National Police of Ukraine, certain **Individuals** created a number of phishing online stores where they offered electronics, mobile devices, computers, and other equipment at discounted prices on condition of payment in advance.

To create the impression of genuine store managers, as soon as the criminals received orders from gullible customers they called them back from a make-believe "call center" and convinced them that the product was located in some other city, meaning that it could be delivered only by post on condition of full payment in advance.

Buyers who fell for this scam entered their bank card details into a website form or transferred funds using the account details provided by the criminals, who then collected the money and broke off all contact.

3 Access: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zhyteliv-odesy-v-internet-shaxrajstvi-z-prodazhu-elektronnoyi-ta-orgtexniky-3473

3.9.8. Auction fraud



Criminals also mask their fraudulent activity by creating fake auctions or using compromised online auction accounts to offer a certain product for sale.

When the buyer's auction bid wins, the buyer pays the price but never receives the product.

Example 3.9.8.1.

Misappropriation of funds through compromised online auction accounts[4]

According to the Cyberpolice Department of the National Police of Ukraine, **Individuals** used compromised accounts to gain access to payment data of users and then used them to shop online.

Criminals hacked accounts of users of online auctions that sell goods. The suspects used compromised accounts to extract payment system credentials (payment details). The perpetrators used these details to shop online.

Individuals also bought compromised social network accounts on DarkNet. They would then secretly log into the accounts and buy advertising for which the victims' cards were charged. The criminals received profit from intermediaries selling the ads.

After a preliminary examination of seized computers, police officers discovered compromised access credentials for personal computers and social network accounts of several thousand citizens of Czech Republic, Italy, France, Germany, Estonia, Spain, the United Kingdom, Poland, and other countries.

4 Access: https://cyberpolice.gov.ua/news/policzejski-bukovyny-vykryly-zlovmysnykiv-u-zlami-akauntiv-internet-aukczioniv-dlya-pryvlasnennya-groshej-gromadyan-1341

3.9.9. Investment fraud schemes

Equally alarming is the growing number of investment fraud schemes in which victims are led to believe that products or services are offered by certain entities.

Criminals steal the identity of well-known companies to bring to life their fraudulent schemes and spread misinformation.

A very common scam involves stealing money from people under the guise of investments through websites created especially for this purpose. The websites promise users profit through trade in bank metals, foreign currencies, crypto currencies, securities, and other assets. "Investors" are misled by an imitation of a program interface that shows purchase and sale transactions and make-believe profit growth by 100 times of their investment or more. When victims request to withdraw their earnings, the "investors" receive calls from fake representatives of the trading platforms at scam call centers, who ask the victims to pay a service fee and a withdrawal commission. The victim is required to pay an additional 15-20% of the amount of their "earnings".

Once the victim pays, the "investor" account gets blocked and the scammers pocket the account balance.

Example 3.9.9.1.

Document forgery to conceal the origin of cash

The SFMS has exposed a scheme in which customer forged documents presented to the bank as proof of the origin of cash.

A financial investigation revealed that **Individual A** deposited a large amount of cash into his own account. To prove the origin of these funds, **Individual A** submitted to **Bank A** a contract for the sale of their own apartment to **Individual B**, in which the sale price exceeded the market price of such real estate several times over.

In order to prove the origin of funds used to buy the apartment, **Individual B** presented contracts for the purchase and sale of securities, under which **Individual B** sold his securities to **Individual C**; the securities were deposited in a securities account with **Bank B**.

Meanwhile, according to information obtained from **Bank B**, **Individual C** never opened the securities accounts mentioned in the purchase and sale contracts. It was also established that the person in question worked a blue-collar job at one of the plants, which does not generate enough income to buy securities worth UAH half a million.

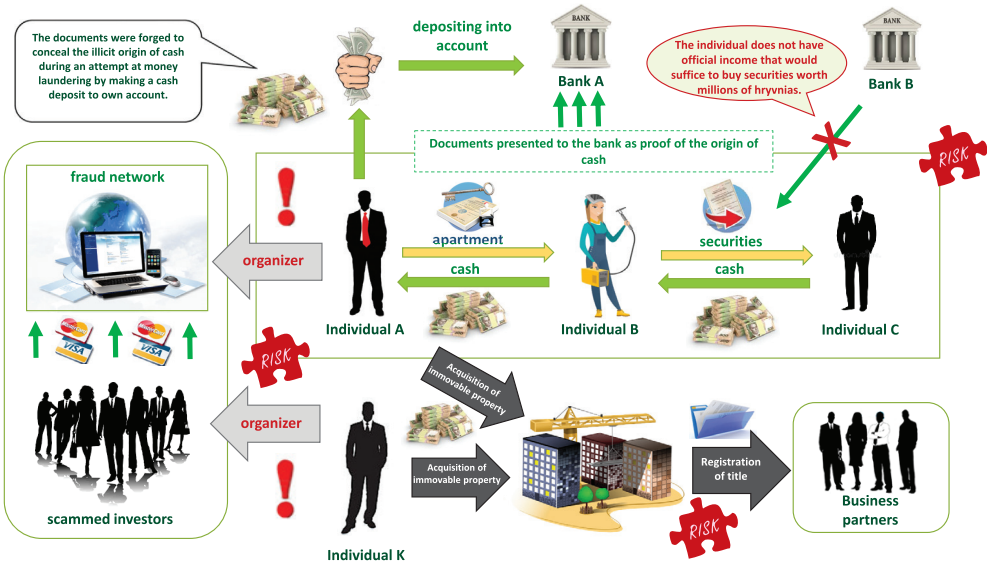
According to the law enforcement, **Individual A** is one of the organizers of a fraudulent scheme that involves stealing funds from individuals in various countries through web resources that purportedly

allow users to make super-profits by trading in various assets (bank metals, crypto currencies, stocks, etc.), and subsequently misappropriating these funds through a chain of controlled companies.

Individual A forged the documents submitted to the banking institution in order to conceal the illicit origin of cash in an attempt to launder them by depositing them into his own account.

Notably, the apartment that **Individual B** bought from **Individual A** is encumbered with a mortgage, which **Individual B** allegedly received from another individual who is a business partner of **Individual A**. As a result of this, **Individual B** is unable to dispose of real estate registered in his own name, which could be an indication that the change of the real estate owner was fictitious and the contract was executed solely for the purposes of money laundering.

Moreover, the investigation revealed that Individual A along with another organizer of the fraudulent scheme **(Individual K**) used the funds stolen from defrauded investors to buy a large quantity of real estate and used fictitious mortgage agreements to register some of the properties in the name of their business partners in order to avoid detection.



Example 3.9.9.2.

Fraud committed by exploiting a bank's trademark

According to the security system of a bank, a new fraud scheme has been detected: unknown individuals registered a website in the USA and illegally use the bank's logo and identity.

It is a scam site that uses links to fictitious investment projects and companies without their consent and makes illegal use of the identity of the bank and other legal entities.

It has been reported that scammers lure victims to join the scam project using promises of high earnings based on a Ponzi scheme with the use of social engineering and presumed hacking. The one-way communication channel of this "project" also speaks to the criminal nature of the scheme: once the victim has filled out the form, the scam operator contacts them to implement the fraud scheme.

3.10. Laundering of proceeds from cybercrimes

Cybercriminals are constantly inventing new ways to commit crimes with the aid of malware.

The most widespread varieties of malware are trojans, ransomware, viruses, worms, and banking malware. The one thing that all of these malware varieties have in common is the malicious intent of their creators or operators.

Specially designed emails with dangerous attachments proved to be an effective and cheap way to hack victims' computers and accounts. All the criminals needed to accomplish this was a single haphazard click from the user.

In many other cases, users fall prey to phishing sites, accidentally reveal the details of their electronic payment instruments or passwords for websites or mobile banking.

Criminals distribute (sell, disseminate) information about compromised accounts in wholesale batches.

Cybercrimes include crimes punishable under the articles of **Section 16 "Crimes committed with the use of electronic computing machines (computers), computer networks, or wired telephony networks" of the Criminal Code of Ukraine**, specifically:

- Article 361 "Unauthorized tampering with the operation of electronic computing machines (computers), automated systems, computer networks, or wired telephony networks" of the Criminal Code of Ukraine.
- Article 361[1] "Creation of malicious software or hardware with the intent to use, distribute, or sell it" of the Criminal Code of Ukraine;
- Article 361[2] "Unauthorized sale or distribution of classified information stored in electronic computing machines (computers), automated systems, computer networks, or on media storing of such information" of the Criminal Code of Ukraine;
- Article 362 "Unauthorized tampering with information processed in electronic computing machines (computer), automated systems, computer networks, or stored on media with such information, committed by a person authorized to access it" of the Criminal Code of Ukraine;
- Article 363 "Violation of the rules governing the operation of electronic computing machines (computers), automated systems, computer networks, or wired telephony networks, or of the procedure or rules for the protection of information handled in them" of the Criminal Code of Ukraine;
- Article 363[1] "Tampering with the operation of electronic computing machines (computers), automated systems, computer networks, or wired telephony networks by sending mass electronic messages" of the Criminal Code of Ukraine.

Below are common examples of investigations into laundering of proceeds from cybercrime.

Example 3.10.1.

Theft of funds of nonresident companies through a hacker attack

Acting on a lead from a foreign financial intelligence unit, the SFMS exposed a fraudulent scheme used to steal funds of nonresident companies.

As a result of the hacker attack, the funds of **Nonresident company A** were debited and transferred to the account of **Company U** with **Bank 1**.

The client's account showed unusually fast movement of funds "in transit". Foreign-currency funds received from **Nonresident company A** were transferred to accounts of a group of companies with other banks as soon as the foreign-currency proceeds were sold.

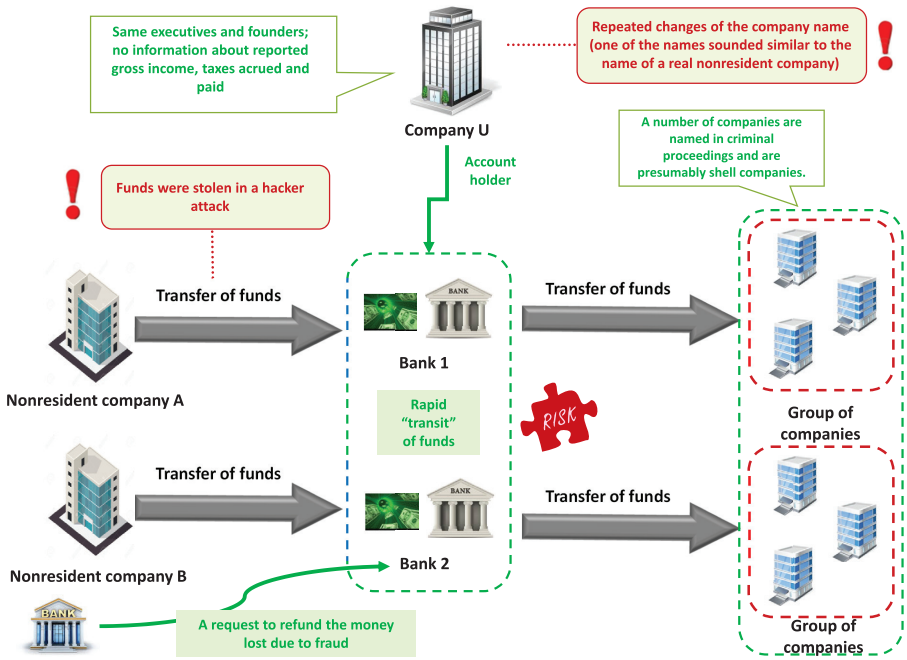
The bank established a business relationship with the client recently (fewer than three months prior), and the bank was unable to reach the client using the contact details provided.

Moreover, a foreign currency transfer from **Nonresident company B** was credited to the account of **Company U** with **Bank 2**. At the same time, an inquiry about suspected fraudulent activity by **Company U** was received from a foreign bank. The funds received in this way were eventually forwarded to a group of presumably shell companies. A number of these companies were named in criminal proceedings.

Notably, **Company U** changed its name a few times, and one of the names sounded similar to the name of a real nonresident company.

Company U has the same executives and founders, and there is no information about reported gross income, taxes assessed and paid.

The law enforcement agency is conducting a pre-trial investigation.



Example 3.10.2.

Theft of assets of a nonresident company through unauthorized debiting of funds

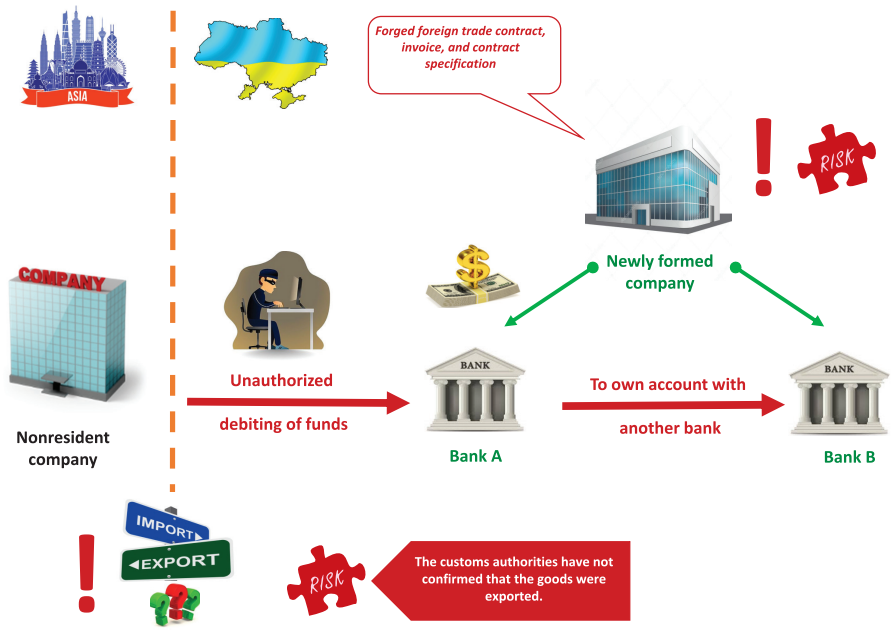
A financial investigation by the SFMS exposed a fraudulent scheme aimed at misappropriation of monetary assets by the **Newly-formed company** through unauthorized debiting of funds from the account of the **Nonresident company**.

The newly-formed company attempted to transfer funds from its own account with **Bank A** to another account of this company with **Bank B**. To this end, **Bank A** was presented with a forged foreign trade contract, invoice, and contract specification as proof of the source of origin of funds in the account of the newly formed company.

Notably, the customs authorities have not confirmed that the goods were exported.

It is noteworthy that the **Newly formed company** does not manufacture the goods named in the specification; during its state registration the founders used the name of a famous brand of a foreign company in order to commit fraud and misappropriate funds of individuals or legal entities acting in good faith.

The law enforcement agency is conducting a pre-trial investigation.



Example 3.10.3.

Theft of money from companies with the use of malware

The National Police of Ukraine has exposed a criminal group that stole funds from bank accounts of legal entities with the use of malware.

A financial investigation revealed that the criminals created and modified malware which they used to access e-payment banking applications such as "Client-Bank" and "Internet Client-Bank". Malware was sent to email addresses of various businesses.

After planting it on the hardware, the criminals monitored money transfers to bank accounts, then tampered with the applications, and illegally transferred funds to accounts controlled by them.

The police initiated a criminal proceeding under part 5 of Article 185 (Theft), part 2 of Article 361-1 (Creation of malicious software or hardware with the intent to use, distribute, or sell it), part 2 of Article 361 (Unauthorized tampering with the operation of computers, automated systems, computer networks, or wired telephony networks), part 3 of Article 209 (Legalization (laundering) of the proceeds of crime) of the Criminal Code of Ukraine.

3.11. Commission of crimes and money laundering with the use of virtual assets

While the latest technologies, products, and related services have the potential to stimulate financial innovation and efficiency and to improve financial services, they also create new opportunities for criminals and terrorists as they can be used for money laundering or financing of their illicit activities.

Virtual assets rely on innovative technologies for rapid transfer of value all over the world and offer multiple potential advantages, including faster and cheaper payments.

Payment products and services based on virtual currencies pose risks of money laundering and terrorism financing on a grand scale. This technology allows anonymous money transfers on a worldwide scale.

Advantages of crypto currencies:

- the open code of the algorithm enables anybody to mine crypto currencies;
- transactions are anonymous (there is no information about the owner of the crypto currency wallet; only the wallet address is available);
- there is no centralized digital bank;
- it is impossible to monitor transactions and payments.
- funds are stored in a decentralized manner, i.e. in the wallets of millions of users worldwide. The same advantages are also disadvantages of crypto currencies, as they make this financial instrument highly vulnerable to speculative trading as well as use in criminal activities such as human trafficking, drug trafficking, terrorism financing, etc.

Virtual currencies that ensure the anonymity of both users and transactions enable criminals to transfer their illicit proceeds quickly from one country to another. They are widely used in the criminal world and enjoy high demand.

A virtual currency can be converted into a national ("fiat") currency or can be unconvertible.

Currencies minted by a number of computer game administrators are unconvertible because they can be used exclusively within the context of the game (such as Warhammer).

Such virtual currencies as Bitcoin can be converted into fiat currencies. That is why convertible virtual currencies usually end up in the hands of criminals and, as a result of this, attract the attention of law enforcement.

Since crypto currencies are largely anonymous, convenient to use, and global in their nature, some of the world's largest criminal groups are interested in using them for money laundering.

The anonymity afforded by virtual assets also attracts criminals who use such assets to launder proceeds from a variety of crimes such as drug trafficking, arms contraband, fraud, tax evasion, cyberattacks, sanction evasion, exploitation of children and human trafficking.

FATF Recommendation 15 requires that VASPs be regulated for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes, that they be licensed or registered, and subject to effective systems for monitoring or supervision.

The EU is taking far-reaching measures to combat money laundering and terrorist financing, specifically efforts to implement tighter controls over crypto currency transactions.

A traditional money laundering technique in this sector involves using proceeds of crime to purchase various virtual assets (crypto currencies). Stage two involves using various exchanges and mixer services to split up the original coins and convert them into other crypto currencies.

In this way, funds can move between hundreds of addresses, thereby making it difficult to track down the original owner. The operating principle of these services is simple: they take crypto currencies from multiple clients, mix them, and eventually produce a mixture that makes it impossible to track down the original owner of money.

In 2021, the British police seized a record amount of crypto currency worth USD 408 million as part of a money laundering investigation.

One of the cryptocurrency trading sites was involved in money laundering.

Virtual currencies can be linked to crimes:

- virtual currency in and of itself can be stolen or obtained by fraudulent means;
- virtual currency can be used to ensure anonymity when buying such items as drugs or firearms;
- virtual currency can be used for blackmail, for instance when a company or institution receives a demand to pay ransom in a virtual currency in order to have malware removed from a computer system;
- virtual currency can be used to launder the proceeds of organized crime or corruption, especially to quickly move assets across borders.

Below are common examples of investigations into money laundering with the use of virtual assets.

Example 3.11.1.

Suspicious transactions using virtual currencies

Acting on a lead from a foreign FIU, banking institutions, and databases, the SFMS detected a group of Ukrainian citizens who carried out suspicious transactions using virtual currencies.

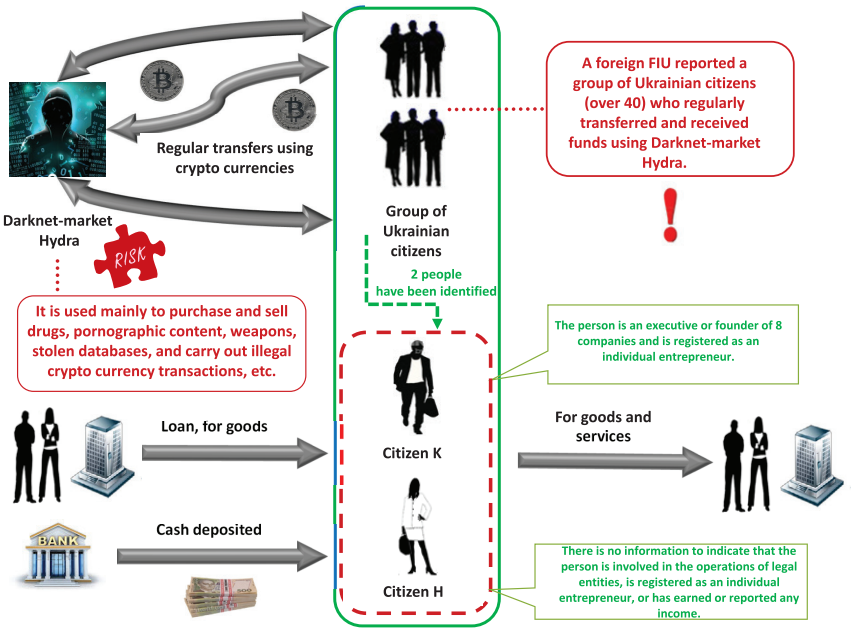
Specifically, a foreign FIU reported **a group of Ukrainian citizens** (over 40) who regularly transferred and received funds using **Darknet-market Hydra**.

Notably, the web resource in question is used mainly to buy and sell drugs, pornographic content, weapons, stolen databases, and carry out illegal crypto currency transactions, etc.

The investigation identified **two individuals** belonging to this group. Notably, **Citizen K** is an executive or founder of 8 companies and is also registered as IE. Also, there is no information to indicate that **Citizen H** is involved in the operations of any legal entities, is registered as an entrepreneur, has earned or declared any income, or has paid any taxes.

Banking institutions sent a number of reports to the SFMS about financial transactions carried out by **Citizen K** and **Citizen H**, including with the use of cash that was presumably earned through illicit operations on the illegal website.

The law enforcement agency is conducting a pre-trial investigation.



Example 3.11.2.

Cybercrimes committed with the use of the Binance cryptocurrency exchange[5]

A law enforcement agency reported detecting transnational criminal activity by a group of individuals who used remotely controlled malware to access ActiveDirectory (AD, software for remote computer management in the Microsoft operating system) on servers of Korean companies.

The criminals then proceeded to install the Clop ransom ware in order to lock data and demand ransom for unlocking the data. The cyber attack against four Korean companies resulted in the blocking of 810 on-premises servers and personal computers.

The investigation revealed that this cyber attack originate from a server with an IP address that is physically located in Kharkiv.

It was established that the crime was committed by an Individual who uses crypto currency wallets on the Binance exchange that received money as ransom for the unlocking of data.

The investigation revealed that the Individual carried out financial transactions and other contracts involving monetary funds and other assets obtained illegally. Without an official income that would be comparable to the amounts spent by him, this individual bought vehicles, valuable real estate, land, and other assets.

The police initiated a criminal proceeding under part 2 of Article Article 209 "Legalization (laundering) of the proceeds of crime", part 2 of Article 361 (Unauthorized tampering with the operation of electronic computing machines (computers), automated systems, computer networks, or wired telephony networks) of the Criminal Code of Ukraine.

Example 3.11.3.

Theft of account identity on the Binance cryptocurrency exchange[6]

The police discovered that an individual tampered with the victim's personal computer, which resulted in the loss of funds.

Specifically, criminals used the victim's account with the Binance exchange to steal USD 60,000 worth of crypto currency.

5 Access: https://reyestr.court.gov.ua/Review/98093620
6 Access: https://reyestr.court.gov.ua/Review/89612547

Example 3.11.4.

Creating online resources for money laundering and terrorism (separatism) financing using virtual assets

The Security Service of Ukraine has put an end to a criminal group that specialized in money laundering and illicit money transfers, including with the use of crypto currencies.

The organizers created a number of online resources (websites, Telegram channels) that enabled users to convert crypto currencies into cash in large amounts (worth over UAH 240 million).

The same service was also used by individuals who supported terrorism and separatism. The transactions were carried out through banned foreign e-money systems. The criminals laundered the money by investing in real estate, land, and precious metals.

Example 3.11.5.

Use of cryptocurrency to pay for drugs

The Security Service of Ukraine uncovered a drug laboratory making amphetamine in Odesa Region. **The criminals** also smuggled MDMA (a semi-synthetic psychoactive compound in the class of amphetamines) from the Netherlands.

Criminals made active use of the Bitcoin cryptocurrency to make payments.

The relevant amount in Bitcoin was deposited in the seller's electronic wallet. The anonymous chat system "Jabber" was used to give the seller a digital code needed to access the funds.

Clients looking to buy drugs or psychotropic substances bought Bitcoin using cards of Ukrainian banks through a variety of crypto currency trading sites.

Example 3.11.6.

Use of cryptocurrency to fund separatist rallies, acts of terrorism, diversion, and extremism

As part of a criminal proceeding initiated in Khmelnytskyi Region under Article 110 "Infringement on the territorial integrity and inviolability of Ukraine" of the Criminal Code of Ukraine, the Security Service of Ukraine exposed a resident of the region who received a reward in Bitcoin for carrying out criminal instructions from officers of intelligence services of a foreign state.

SECTION IV. COMMON INSTRUMENTS, INDICATORS, AND METHODS OF MONEY LAUNDERING AND TERRORISM (SEPARATISM) FINANCING

The broad variety of organizational structures of criminal groups, constant adaptation by criminals to methods and techniques used to combat ML/TF/PF by the international community, and the criminals ability to quickly adapt to external changes make it safe to state that the instruments, techniques, and methods employed to commit crimes are constantly evolving.

Based on the study findings, the SFMS has summarized the most common indicators that help detect schemes linked to money laundering and terrorism (separatism) financing.

In order to properly implement the risk-based approach, entities involved in AML/CFT can expand the list of indicators used to detect suspicious financial transactions (activities).

Principal instruments used in the existing money laundering schemes

The study findings helped identify the following principal instruments used in the most common money laundering schemes:

- use of cash;
- overstatement or understatement of the cost of goods, work, or services;
- transit transactions;
- transactions without commodities;
- substitution of official product names;
- failure to repatriate foreign currency earnings;
- no payments under import contracts;
- use of fictitious contracts;
- extending/repaying financial aid;
- transactions involving securities, including so-called "junk" bonds;
- acquisition of corporate rights;
- assignment of receivables (factoring);
- insurance against financial risks;
- co-investment in construction projects;
- re-registration of assets under the name of business partners;
- use of forged documents;
- purchase of real estate and executive cars;
- use of e-money and instant transfer systems;
- use of trading operations for money laundering;
- illegal services provided through professional networks with money laundering;
- crypto currency transactions;
- use of the mechanism of "counter cash flows";
- payment of agency fees;
- use of malware;
- duplicate transactions performed by the cashier;
- data theft;
- hacking of user accounts;
- use of skimmers on terminal devices;
- creation of clone companies;

- use of frontmen (figureheads);
- use of "junk bonds";
- social engineering;
- use of complex insurance payout conditions.

Indicators of suspiciousness of participants

The study findings helped identify the following principal indicators of suspiciousness of participants present in the most common money laundering schemes:

- short work experience (duration of operations), date and place of registration;
- no hired employees or a small staff;
- same founder and executive officer;
- the founder or manager is a person who belongs to socially vulnerable groups (students, retirees, individuals receiving social benefits, etc.), individuals with a special status (underprivileged persons, beggars), young people (up to 20 y.o.) or elderly people (over 75 y.o.);
- the founder or manager is a person registered and residing in territories outside the control of Ukraine (temporarily occupied territories of Donetsk and Luhansk regions, the Autonomous Republic of Crimea and the city of Sevastopol);
- companies registered in offshore jurisdictions or areas with ongoing armed conflicts;
- the legal entity frequently changes its name or the list of founders and executives;
- individuals are ultimate beneficial owners or acts as founders or executives at a large number of legal entities;
- small charter capital;
- lack of fixed assets, production facilities, warehouses, other assets;
- liquidation of a business entity as soon as payment has been processed;
- not a manufacturer of goods;
- no wages accrued or paid to employees;
- no licenses or permits for specific types of activity;
- no declared income or paid taxes;
- no rent payments;
- the client or the client's contracting parties are named in criminal proceedings;
- documents contain gross errors, contradictions, or signs of forgery;
- false UBO;
- a director, accountant, or founder is involved in the operations of numerous legal entities;
- one and the same group of entities or individuals are participating in the majority of competitive bidding auctions;
- there are court rulings against founders or executives of companies in which they were found guilty of submitting forged documents upon registration;
- the name of the legal entity coincides with names of well-known international companies;
- past-due taxes;
- registration at an address of multiple registrations;
- payments expected in the ordinary course of business are not being made against invoices;
- the number of full-time employees of a legal entity is disproportionate to the liabilities of the legal entity;
- negative reports in the public domain.

Indicators of suspiciousness of financial transactions (activities)

The study findings helped identify the following principal indicators of suspiciousness of financial transactions (activities) present in the most common money laundering schemes:

- unjustifiably large amounts of cash used for payments;
- transit movement of non-cash funds through the account (funds leave the account shortly after being credited to it);
- a party to a financial transaction fails to offer explanations regarding financial transactions and the apparent signs of concealment of the source of funds;
- the amount of reported income is disproportionate to the amounts of financial transactions;
- a history of forgery of official documents;
- complaints filed by victims with the police;
- available information about an ongoing criminal proceeding or judicial prosecution of a party to a financial transaction;
- financial transactions carried out without an apparent purpose;
- financial transactions with a large number of contracting parties (transactions do not match the business profile; assets are scattered in order to conceal cash flows);
- financial transactions to top up a large number of mobile phone accounts;
- an individual is carrying out commercial (trade) operations without declaring their entrepreneurial status to the authorities;
- there are no standard payments made through accounts of IE or legal entities that one would normally expect in the due course of business (rent, utilities, taxes, duties, etc.);
- failure to disclose information in the details of payment about the reason for and purpose of the transfer of funds;
- spontaneous turnovers through accounts of a legal entity (substantial turnovers or total absence of turnovers);
- use of presumably shell companies;
- creation of companies that are "clones" of a well-known foreign company;
- regular transfers of funds to accounts of legal entities as payment under a factoring agreement, assignment of receivables or loans;
- financial transactions under presumably sham insurance contracts;
- financial transactions involving securities that show signs of being "junk bonds";
- large daily turnovers with a small opening and closing balance;
- funds credited to and debited from accounts of an individual with a large number of counterparties despite the fact that this individual is not registered as an entrepreneur;
- structured payments;
- payments without naming a specific product or service;
- questionable financial transactions among a group of legal entities located at addresses of mass registrations;
- a party to a financial transaction is a person who was involved in activities of illegal paramilitary groups;
- an obvious discrepancy between the details of credit and debit transactions and the client's financial operations;
- financial transactions involving trade in minerals in the absence of mining licenses or permits or when the origin of such minerals is unconfirmed;
- acquisition of costly assets using money from unconfirmed sources;
- cash transactions worth millions of hryvnias without any officially declared income.

Methods of money laundering

The study findings helped identify the following principal methods of money laundering and terrorism (separatism) financing:

- depositing of cash into several accounts with different banking institutions using the same documents to prove the origin of funds;
- money laundering through acquisition of costly assets;
- extending financial aid to an affiliated company, which is later returned and withdrawn as cash;
- the winning bidder transfers public funds to a number of IEs with the details of payment indicated as "payout of income", whereas the period of activity of such IEs is limited to the period during which public funds are disbursed;
- a state company (or publicly funded institution) transfers funds to a business entity although no goods have been supplied or services rendered;
- public funds are received by business entities without hired workers and production facilities, which subsequently transfer some of the funds to intermediaries towards performance of the terms of the tender. The remaining funds are converted into cash or transferred to accounts of presumably shell companies as financial aid, payment for securities, assignment of debt with the ultimate objective of collecting cash, or are transferred to accounts of companies that carry out transit transactions;
- forgery of documents used to prove the origin of cash;
- export operations without payments;
- import operations without payments;
- siphoning of funds out of Ukraine by forging import contracts and performing fictitious imports;
- use of the mechanism of "counter cash flows" to conceal cash conversion with the aid of wholesalers and retailers;
- crediting of funds to accounts of IEs with subsequent conversion into cash;
- siphoning of funds out of a business in the real sector of the economy by entering into sham insurance contracts with an insurer;
- financing of terrorism and separatism through contraband coal shipments from the temporarily occupied territories of Donetsk and Luhansk Regions;
- transfer of funds to NGOs in the form of grants and aid designed to potentially finance terrorism (separatism);
- theft of funds of legal entities using a fraudulent scheme that involves sending presumably fake payment claims to Ukrainian banking institutions demanding debt recovery;
- companies cloned to resemble well-known manufacturers steal funds of nonresident companies and promptly transfer the funds to accounts of presumably shell companies;
- use of card accounts of individuals to receive proceeds from illicit trafficking of drugs or psychotropic substances, weapons or pornographic videos, followed by cash withdrawals or transfers to other identified or unidentified individuals.

Most common methods of financing of terrorism and separatism

- transfer of funds via international e-money system (Zolota Korona, Yandex Money, Money@mail.ru QIWI, WesternUnion, MoneyGram, PayPal, Webmoney), electronic and web wallets;
- cash couriers;
- providing material resources to terrorist groups through nonprofit (charitable) organizations controlled by such groups or individuals;
- international shipments with payments made in the territory of third countries;
- financing of terrorism by nonresidents under the guise of legitimate activities;
- voluntary donation of cash by individuals to representatives of terrorist and/or separatist organizations;
- transfer of funds to card accounts of members of terrorist groups;
- use of fictitious financial structures to withdraw cash;
- use of third parties to collect cash;
- use of ATMs to withdraw cash from bank accounts of third parties;
- use of debit cards;
- taking out loans without the intention of repaying them;
- using mutual setoffs to conceal cash flows;
- transfer of property and other assets directly to individuals complicit in terrorism;
- extortion of financial aid from business entities for the purpose of subsequent funding of terrorism and separatism, including by leaders of paramilitary groups operating in the temporarily occupied territories of Donetsk and Luhansk regions;
- armed robberies, burglaries, kidnappings for ransom;
- unauthorized debiting of funds from accounts of legal entities, followed by subsequent transfers to accounts of individuals or legal entities.

CONCLUSION

The findings of the typologies study indicate growing threats of fraud, cybercrime, and misappropriation of public funds in the conditions of the COVID-19 pandemic.

As the number of remote financial transactions increases, so does demand for online trading platforms and virtual assets for payments, as well as for financial transactions outside the limits of the national financial system.

The vulnerabilities that arise are chiefly due to the nonexistent or nearly impossible control over financial transactions, and more specifically: ineffective detection of crimes by individuals who provide services outside the financial system of the country, ignorance, unawareness, and gullibility of citizens who use online services, as well as the use of the latest technologies and lack of proper regulation of virtual assets.

The use of this typological study while analyzing financial flows can help paint a complete picture of the algorithm of money laundering or other crimes. Detecting such schemes requires obtaining broad access to all sorts of information, identifying the list of discrepancies with official data, as well as systematizing the findings of this analysis.

ANNEX. ANALYTICAL TOOLS FOR CONTROL AND MONITORING

1. Analytical tools

Reporting entities use the following sources of information in their activities:

- data from state registers;
- data from open sources in the public domain;
- information from law enforcement agencies;
- online services for verification of companies;
- findings of journalistic investigations;
- official documents of the SFMS and state financial monitoring entities;
- etc.

In order to conduct a customer due diligence at the onboarding stage as well as carry out a more detailed in-depth analysis as part of the monitoring of financial transactions while providing services to customers, reporting entities also use:

- in-house scoring models to prevent the onboarding of suspicious customers;
- in-house scoring models for assessing the risk of business relations with the customer depending on the type of customer (legal entity, individual, IE);
- existing matrices for assessing the level of risk associated with politically exposed persons;
- scoring models for detecting potentially high-risk customers;
- various reports and in-house scenarios for screening out suspicious financial transactions (activities).

In order to detect suspicious transactions, reporting entities create the appropriate rules for screening out transactions based on the following fields: transaction date, details of payment, amount, risk level, country, information about the type of account, etc.

Such entities also carry out scenario analysis that includes studying the turnaround of assets in general and specific financial transactions of customers over time.

Reporting entities supplement their in-house analytical systems with additional information about parties to transactions and other details, which may substantially expand the scope of data that needs to be analyzed.

Detection of financial transactions subject to financial monitoring with the use of automated systems that include analysis of the risk criteria and indicators of suspiciousness of financial transactions (among other factors) is of utmost importance for the accomplishment of objectives of a reporting entity.

Example of details for building a scenario for screening out suspicious financial transactions (activities)

Relating to the customer's profile:

- size of the charter capital of a business entity;
- type of activity of the business entity;
- number of employees of the business entity;
- amount of income and taxes paid by the business entity;
- period during which the business entity has been active/age of the individual;
- information about the ultimate beneficial owner, founders and executives of the business entity and their involvement in the operations of other legal entities;
- information about changes of the ultimate beneficial owner and founders or executives of the business entity;
- any information about ongoing criminal proceedings and investigations into commercial crimes against the owner of a material interest/controller or legal entity, its managers and/or representatives;
- availability of production facilities, warehouses and retail outlets, other assets needed to conduct the official commercial activities of the business entity;
- potential amount of funds (turnover) available to the business entity through the specific service (product).

Relating to the customer's financial transactions:

- number of accounts of payment cards of a business entity;
- comparison of the amounts of debit and credit transactions through the account of the business entity during one day/specific period;
- changes in amounts of financial transactions through accounts of a business entity;
- nature of financial transactions carried out;
- information about the use of a safety deposit box by a business entity;
- IP addresses used to carry out financial transactions of the business entity.

2. Public information resources of supervisory (state) authorities and private organizations

The use of automated procedures for collecting and analytical processing of information from open sources is an important step towards supporting management decisions and boosting the level of efforts to combat ML/TF/PF.

Obtaining additional information from public informational resources of the supervisory (state) authorities and private organizations is essential to analyzing the existing ML/TF/PF schemes.

The SFMS is working consistently to detect public sources of information that can be used as a source of additional data. Helpful links are provided according to the topics of the study.

Some helpful links are provided in typologies studies of the SFMS for past periods, which are available in the public domain.

Listed below are current open sources covering a broad range of issues.

2.1. Terrorism

Terrorism

SFMS	List of individuals involved in terrorist activities or subject to international sanctions
https://fiu.gov.ua/pages/dijalnist/protidija-terorizmu/perelik-teroristiv	

"Myrotvorets" website	Center for the study of suspected crimes against national security of Ukraine, peace, security of mankind, and international law and order
https://myrotvorets.center	

US Department of State	List of countries supporting terrorism
https://www.state.gov/ country-reports-on-terrorism-2/	

2.2. Lists of the UN Security Council

Consolidated List of the UN Security Council

UN Security Council	
https://www.un.org/securitycouncil/content/un-sc-consolidated-list https://scsanctions.un.org/search/	Consolidated list of individuals and legal entities subject to sanctions instituted by the UN Security Council

2.3. Information about individuals

Information about individuals

Ministry of Internal Affairs of Ukraine	
http://wanted.mvs.gov.ua/searchperson	Individuals wanted by the authorities

2.4. Politically exposed persons

Politically exposed persons

Clause 6 of Annex 9 to Regulation approved by Resolution No. 65 of the Board of the National Bank of Ukraine lists the sources of information that can be used by a bank to decide whether the client belongs to the category of PEPs on condition that the risk level of a business relationship (or one-time financial transaction involving a large amount) with the client is higher than low, specifically:

- databases of service providers that provide information services free of charge or in consideration of a fee;

- public sources of data on the Internet, including official online offices of the state authorities;
- official online offices of systems for income reporting by politically exposed persons, including the Unified state registry of declarations of persons authorized to carry out functions of the state or local government bodies.

Open registry of national politically exposed persons of Ukraine https://pep.org.ua/uk/	Search for national politically exposed persons and people connected to them

Directory "Official Ukraine Today" http://dovidka.com.ua/user/	Contains information about public authorities and bios of government officials

Official web portal of the Verkhovna Rada of Ukraine http://w1.c1.rada.gov.ua/pls/site2/p_deputat_list	Profiles of Ukrainian Members of Parliament

2.5. Declarations of public officers

Declarations of persons authorized to carry out functions of the state or local government bodies

Uniform state registry of declarations https://public.nazk.gov.ua/	Unified state registry of declarations of persons authorized to carry out functions of the state or local government bodies

"Declarations" project https://declarations.com.ua/	Database of declarations of public officers

2.6. Verification of the validity of documents

Verification of the validity of documents

State Migration Service of Ukraine (SMSU)	
https://nd.dmsu.gov.ua/	Database of invalid, stolen, or lost IDs

Ministry of Internal Affairs of Ukraine (Unified State Portal of Open Data)	
https://wanted.mvs.gov.ua/passport	Information about stolen, lost, or expired passports of Ukrainian citizens

2.7. Financial sanctions

OFAC

Financial sanctions

US Department of the Treasury	
https://home.treasury.gov/ policy-issues/financial-sanctions/specially-designated-nationals-list-data-formats-data-schemas https://sanctionssearch.ofac.treas.gov/	OFAC publishes a list of individuals or companies that belong to, are controlled by, or act for or on behalf of the designated countries
The list also enumerates specific individuals, groups, and organizations, particularly terrorists and drug traffickers identified as part of programs unrelated to a particular country. These individuals are collectively referred to as "specially designated nationals" or "SDN". Their assets are frozen, and US citizens are typically prohibited from doing business with them.	

2.8. Sanctions imposed by Ukraine

Sanctions imposed by the National Security and Defense Council of Ukraine

National Security and Defense Council of Ukraine	List of individuals or legal entities subject to restrictive measures (sanctions)
https:// sanctions-t.rnbo.gov.ua/	

2.9. Registries of the Ministry of Justice

Automated systems of Unified and State registers created by orders of the Ministry of Justice of Ukraine

Registries of the Ministry of Justice of Ukraine	Published data from Unified and State registers created pursuant to Ukrainian law
https:// nais.gov.ua/ registers	

Cabinet of electronic services	Published data from Unified and State registers created pursuant to Ukrainian law
https:// kap.minjust.gov.ua	

2.10. Construction

Portal of the state electronic system in the construction area

https://e-construction.gov.ua/	The portal of the Unified System in the Construction area is the public segment of the System, which is designed to provide free unobstructed access to data generated in the System for all types of users.

The portal offers convenient information search tools with the ability to project data onto a map, as well as basic analytical tools. The portal also offers helpful online services that can help with the search for information. The portal functionality is being expanded as the Unified System in Construction is evolving.

2.11. Securities

Information about professional securities market participants

Ukrainian Stock Market Infrastructure Development Agency https://smida.gov.ua/	Information published by securities issuers

2.12. Judicial authorities

Registry of court decisions

Registry of court decisions	
https://reyestr.court.gov.ua/	Unified state register of court decisions

2.13. Owners of banking institutions

Information about owners of a significant interest in Ukrainian banks

National Bank of Ukraine	
https://bank.gov.ua/control/uk/publish/article?art_id=6738234&cat_id=51342	Information about owners of a significant interest in Ukrainian banks

2.14. Companies of Ukraine

Registration details of Ukrainian companies

Internet addresses	
https://youcontrol.com.ua https://opendatabot.ua https://clarity-project.info https://vkursi.pro https://zaparkanom.com.ua https://ca.ligazakon.net https://ring.org.ua	Current details and information about operations of business entities registered in Ukraine

2.15. Companies registered in foreign jurisdictions

Resources with information about nonresident companies

OpenOwnership	
https://opencorporates.com/	The world's largest open database of companies
OpenOwnership is an nongovernmental technological initiative providing broader access to information about beneficial ownership. OpenOwnership currently includes data on more than 4.2 million companies. OpenOwnership also provides technical assistance to governments and companies looking to actively disclose information.	

Forbes Global 2000 list	
http://www.forbes.com/global2000/list/#search	Largest companies of the world

Organized Crime and Corruption Reporting Project	
OCCRP https://www.occrp.org/ru/investigations	The database contains information about more than 800,000 offshore companies, foundations, and trusts appearing in the Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers, and Offshore Leaks investigations

The OCCRP regularly publishes topical international journalistic investigations into current money laundering schemes based on document leaks from various public and private entities exposing unofficial activities of corrupt official and organized criminal groups.

Database of offshore leaks	
ICIJ https://offshoreleaks.icij.org	The database contains information about more than 800,000 offshore companies, foundations, and trusts appearing in the Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers, and Offshore Leaks investigations

A global archive of research materials for investigations.

The Aleph data platform stores an archive of current and past databases, documents, leaks, and investigations.

This network helps track down ties, locate stolen funds, expose political influence and corruption.

Dato Capital	Online database of companies and their directors
en.datocapital.com	

The database contains information about companies registered in the Netherlands, the UK, Gibraltar, Spain, Panama, Cayman Islands, Luxembourg, the British Virgin Islands, Malta, and Curacao.

The database offers pay-for and free content.

Free: legal form of organization of a company, date of registration, number, registered office address, active/inactive status, date of the most recent changes.

Fees apply: registration and constitutional documents, appointments/dismissals of directors, taxes paid, financial statements.

Extended report available for a fee: registration documents, powers of attorney, complete list of amendments to the charter, list of documents submitted, registration information with a list of directors and secretaries, company news, information about the company's directors and secretaries with other companies.

Bureau van Dijk Electronic Publishing	A vast database of registration data of companies registered in various jurisdictions all over the world.
https://www.bvdinfo.com/en-gb	

Limited information (legal form of organization, place of business, active/inactive status) is available free of charge using the online search service.

Official Portal for European Data	Free: access to open data published by EU institutions and agencies.
http://data.europa.eu/euodp/en/home	

Open registries with registration data of nonresident companies

Region (country)	Description	Address
European Union	Official Portal for European Data. Free: access to open data published by EU institutions and agencies.	http://data.europa.eu/euodp/en/home
European Union	Register of EU member states (including Iceland, Lichtenstein, and Norway).	https://e-justice.europa.eu/content_find_a_company-489-en.do?clang=en
European Union	Official list of business registers in EU member states.	https://e-justice.europa.eu/content_business_registers_in_member_states-106-en.do?clang=en
European Union	Official list of land registers in EU member states.	https://e-justice.europa.eu/content_land_registers_in_member_states-109-en.do
European Union	Consolidated register of insolvent companies in EU member states.	https://e-justice.europa.eu/content_interconnected_insolvency_registers_search-246-en.do
Austria	Register and data of financial statements of Austrian companies. Contains pay-for content.	https://www.firmenbuchgrundbuch.at/fbgb/easy/fb/search
British Virgin Islands	Data on companies registered in the British Virgin Islands	http://www.bvifsc.vg
United Kingdom	Court Register of the Supreme Court of the United Kingdom.	https://www.supremecourt.uk/current-cases/index.html
United Kingdom	Court Register of Administrative Appeals of the High Court.	https://www.judiciary.gov.uk/about-the-judiciary/who-are-the-judiciary/judicial-roles/tribunals/tribunal-decisions/osccs-decisions/
United Kingdom	Register of UK companies	https://beta.companieshouse.gov.uk/
United Kingdom	Information about a company in the United Kingdom of Great Britain and Northern Ireland, which includes, among other things: (address, date of establishment); current and former company officials; scanned copies of documents (registration, changes of officials, annual reports, etc.); information about encumbrances; previous company names.	https://www.gov.uk/government/organisations/companies-house

Region (country)	Description	Address
United Kingdom	Information about real estate that includes, among others things: information about the property, including the registration of title, number of the document proving the registration of title, information about the owner, purchase price, any rights-of-way through the territory, as well as information on whether mortgage has been paid. Similar registries of real estate are available in Northern Ireland (https://www.nidirect.gov.uk/articles/searching-the-land-registry) and Scotland (https://www.ros.gov.uk/).	https://www.gov.uk/search-property-information-land-registry
United Kingdom	Interactive map and database of owners of foreign companies.	http://www.private-eye.co.uk/registry
United Kingdom	In the United Kingdom, the police may check ownership of a vehicle through the Police National Database (PND). The UK Driver and Vehicle Licensing Agency (DVLA) maintains a record of registered vehicle holders and discloses information about them on "reasonable grounds" even if the person requesting such information is not a police officer.	https://www.gov.uk/request-information-from-dvla
United Kingdom	Ships	http://discovery.nationalarchives.gov.uk/browse/r/h/C3770037.
United Kingdom	The registration of aircraft in the United Kingdom involves keeping a register and using means of identification for British commercial and private aircraft, and the registration marks begin with the identification prefix "G". The register is maintained by the UK Civil Aviation Authority.	http://www.caa.co.uk/Aircraft-register/G-INFO/Guidance-on-using-the-G-INFO-Database/
United Kingdom	The Crown Court is a national court that sits in districts located in the largest cities of England and Wales. It considers all serious criminal cases transferred from magistrate courts. Cases are tried by a judge with the participation of 12 jurors. There are about 90 Crown Courts in England and Wales, including London's Central Criminal Court known as the Old Bailey. The decisions of the Crown Court are considered by the Criminal Division of the Court of Appeal, chaired by the Lord Chief Justice. Appeals from the Court of Appeal are examined by the Supreme Court.	http://www.nationalarchives.gov.uk/help-with-your-research/research-guides/criminal-courts-england-wales-from-1972/

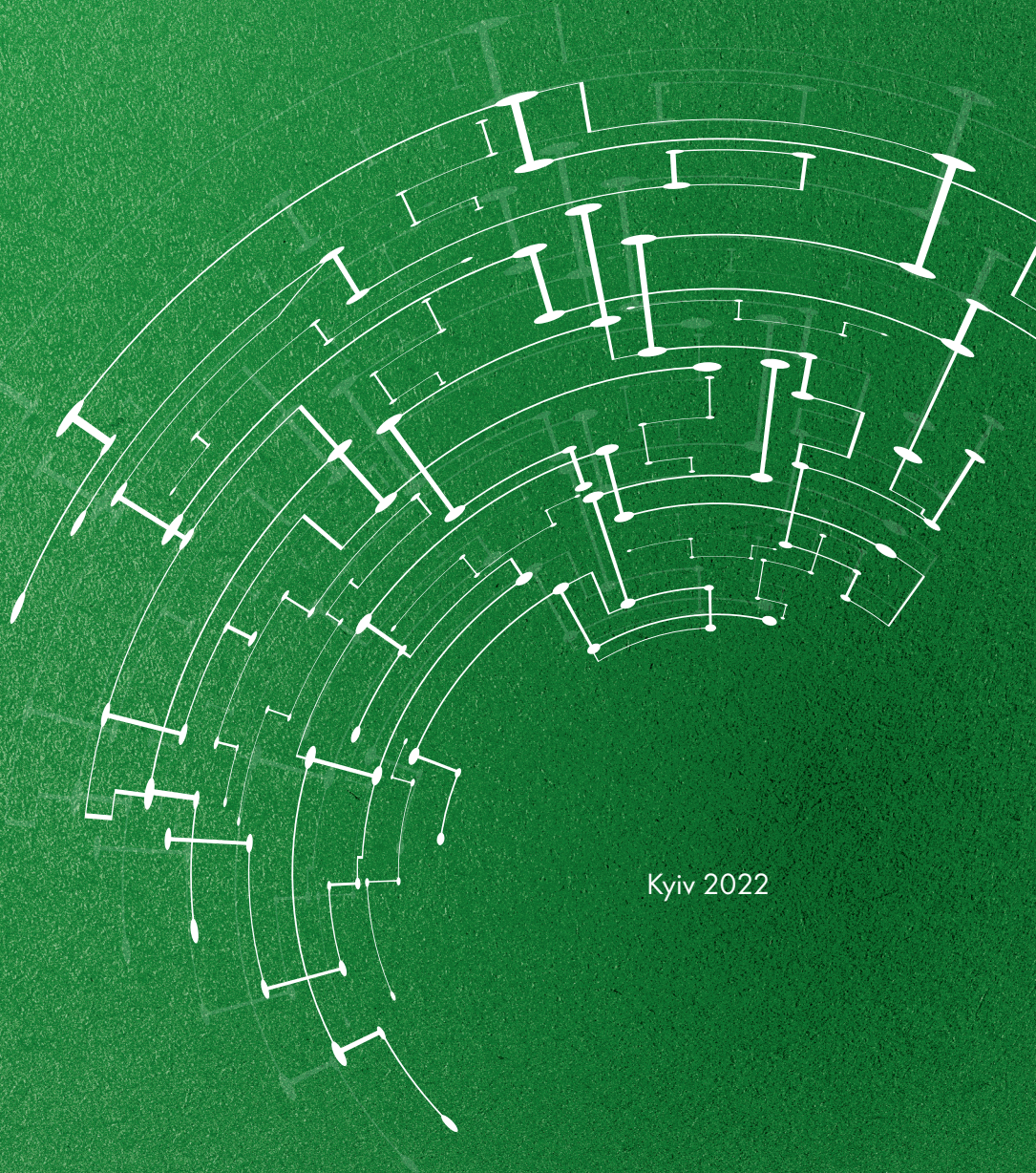
Region (country)	Description	Address
United Kingdom	Court documents. Cases can be searched by the name of the defendant, the name of the court, the offense, or the name of the attorney. The search returns general information, but registration is required to view verdicts. However, this service is provided free of charge.	http://www.thelawpages.com/court-cases/court-case-search.php?mode=1
Great Britain and Northern Ireland	This registration database of the United Kingdom offers the following information free of charge: - details of the company (address, date established); - current and former executives of the company; - scanned copies of documents (registration, changes of executives, annual statements, etc.); - information about encumbrances; - previous names of the company; - information about insolvency; - information about beneficiaries.	https://www.gov.uk/government/organisations/companies-house
Great Britain and Northern Ireland	This registration database of the United Kingdom offers the following information free of charge: - details of the company (address, date established); - current and former executives of the company; - scanned copies of documents (registration, changes of executives, annual statements, etc.); - information about encumbrances; - previous names of the company; - information about insolvency; - information about beneficiaries.	https://beta.companieshouse.gov.uk/
Estonia	Free: name and legal form of organization of the company, registration number of the company, registered office address, size of the charter capital, date of registration and approval of the charter, active/inactive status, dates of submission of details for the register.	https://ariregister.rik.ee/lihtparing
Estonia	Open economic register of Estonia.	www.mtr.mkm.ee

2.16. Information about assets

Aircraft	Aircraft registration database
http://www.airframes.org/	
Free: the registration number of the aircraft can be entered to receive information about the aircraft model, type, owner, date of manufacture, and history. Information about the airline operator can be obtained by entering an ICAO/IATA code.	

Aircraft	Databases of aircraft photos
https://www.planespotters.net/ https://www.jetphotos.com	
Free: the registration number of the aircraft can be entered to view photos of the aircraft, including the date and place where the photos were taken.	

Flight tracking	A global flight tracking service that provides information about aircraft all over the world in real time.
https://www.flightradar24.com https://www.marinetraffic.com/	
Free: plane movement can be tracked in real time by entering the aircraft registration number. Fees apply: past flights of the aircraft.	



Kyiv 2022