

# TYOLOGICAL STUDIES OF THE STATE FINANCIAL MONITORING SERVICE OF UKRAINE

---

**2017**



The State Financial  
Monitoring Service of  
Ukraine



State Financial Monitoring Service of Ukraine

State Institution of Post-Graduate Education "Academy of Financial Monitoring"

# **TYPOLOGICAL STUDIES**

## OF THE STATE FINANCIAL MONITORING SERVICE OF UKRAINE

---

**2017**

**Kyiv 2018**

Recommended by the Inter-branch Scientific and Methodical Council of the State Institution of Post-Graduate Education "Academy of Financial Monitoring"  
(Protocol of 29.01.2018 № 1)



Publication and translation into English was made with the assistance of the European Union Anti-Corruption Initiative (EUACI)



**EUACI** EUROPEAN UNION  
ANTI-CORRUPTION  
INITIATIVE

Typological Studies of the State Financial Service of Ukraine for 2017– K., 2018. – 148 p.

The publication deals with the most common trends and schemes of money laundering and terrorist financing in 2017. In particular, examples of real cases of money laundering and terrorist financing associated with the risks of cash use and the risks of terrorism and separatism are given.

Typological studies include information on the results of the work of state authorities – participants of the national financial monitoring system.

The publication is designed for employees of reporting entities and state financial monitoring entities, law enforcement, intelligence and judicial authorities, as well as scientists and practitioners in the area of financial monitoring.

# CONTENTS

---

Foreword of the Head of the State Financial Monitoring Service of Ukraine Mr. Igor Cherkaskyi . . . .	8
<b>PART I. RISKS OF CASH USE . . . . .</b>	<b>11</b>
INTRODUCTION TO THE FIRST PART . . . . .	12
<b>SECTION I. USE OF CASH IN UKRAINIAN ECONOMY. GENERAL OVERVIEW . . . . .</b>	<b>17</b>
1.1. Overview of cash market trends in Ukrainian economy . . . . .	18
1.2. Use of payment cards . . . . .	21
1.3. Factors contributing to the use of cash . . . . .	23
1.4. Cash transaction threshold values for inter-entity transactions . . . . .	24
1.5. Cash in money laundering . . . . .	27
1.6. Cryptocurrency as a tool in money laundering . . . . .	27
<b>SECTION II. DETECTION OF RISKY CASH TRANSACTIONS . . . . .</b>	<b>29</b>
<b>SECTION III. INTERNATIONAL MONEY LAUNDERING PLATFORMS . . . . .</b>	<b>35</b>
<b>SECTION IV. CONVERSION CENTRES AND THEIR OPERATIONS . . . . .</b>	<b>39</b>
<b>SECTION V. USE OF PRESUMABLY SHELL COMPANIES IN MONEY LAUNDERING OR FINANCING OF TERRORISM . . . . .</b>	<b>51</b>
<b>SECTION VI. BUDGET FUND THEFT WITH FURTHER CONVERSION OF FUNDS TO CASH . . . . .</b>	<b>57</b>
<b>SECTION VII. USE OF CASH BY PEP’S, RELATED PERSONS AND OTHER CIVIC SERVANTS . . . . .</b>	<b>61</b>
<b>SECTION VIII. MONEY LAUNDERING THROUGH REAL ESTATE PROCUREMENTS . . . . .</b>	<b>67</b>
<b>SECTION IX. USE OF CASH IN THE SCHEMES RELATED TO TRADE IN NARCOTIC (PSYCHOTROPIC) SUBSTANCES, THEIR ANALOGUES AND PRECURSORS . . . . .</b>	<b>71</b>
<b>SECTION X. ILLICIT CASH MOVEMENT . . . . .</b>	<b>77</b>

SECTION XI. CASH COMBINED WITH OTHER TOOLS . . . . .	81
CONCLUSION TO PART I . . . . .	83
<b>PART II. RISKS OF TERRORISM AND SEPARATISM . . . . .</b>	<b>85</b>
INTRODUCTION TO THE SECOND PART . . . . .	86
<b>SECTION I. RATIONALE . . . . .</b>	<b>89</b>
<b>SECTION II. TERRORIST-RELATED RISKS AND THREATS. GENERAL OVERVIEW . . . . .</b>	<b>93</b>
2.1. Risks and threats related to terrorism and terrorism financing in Ukraine. Overview . . . . .	95
2.2. World trends to counter terrorism and terrorism financing . . . . .	97
2.3. TF risks related to ISIL’s activities. . . . .	98
2.4. Use of foreign militants in financing of terrorism . . . . .	99
2.5. Counteraction to risks and threats related to terrorism and terrorism financing in Ukraine . . . . .	100
<b>SECTION III. STANDARD METHODS, SCHEMES AND TOOLS FOR TERRORISM FINANCING . . . . .</b>	<b>103</b>
3.1. Use of NPOs in terrorism financing . . . . .	106
3.2. Indirect terrorism financing . . . . .	111
3.3. FT sources . . . . .	113
3.4. Illicit funds in terrorism financing. . . . .	115
3.4.1. Use of proceeds earned from drug trafficking in terrorism financing . . . . .	115
3.4.2. Use of proceeds from credit card fraud in terrorism financing . . . . .	116
3.4.3. Use of proceeds from cheque fraud in terrorism financing . . . . .	117
3.4.4. Use of proceeds from extortion in terrorism financing . . . . .	117
3.4.5. Use of various sourced illicit proceeds for terrorism financing . . . . .	118
3.5. Movement of funds to finance terrorism. . . . .	119
3.5.1. Use of a state financial system in terrorism financing . . . . .	120
3.5.2. Use of trade in terrorism financing . . . . .	122
3.5.3. Use of payment systems in terrorism financing. . . . .	125
3.5.4. Use of cash transporters (cash couriers) for terrorism financign . . . . .	129
3.6. Emerging terrorist risks . . . . .	130
3.6.1. Fundraising with the use of social networks in terrorism financing . . . . .	130
3.6.2. Use of virtual currencies in terrorism financing. . . . .	132
3.6.3. Use of prepaid cards for terrorism financing. . . . .	134
3.6.4. Use of revenues from the exploitation of natural resources and mineral deposits for terrorism financing . . . . .	135
3.6.5. Use of the oil and gas industry for terrorism financing . . . . .	137



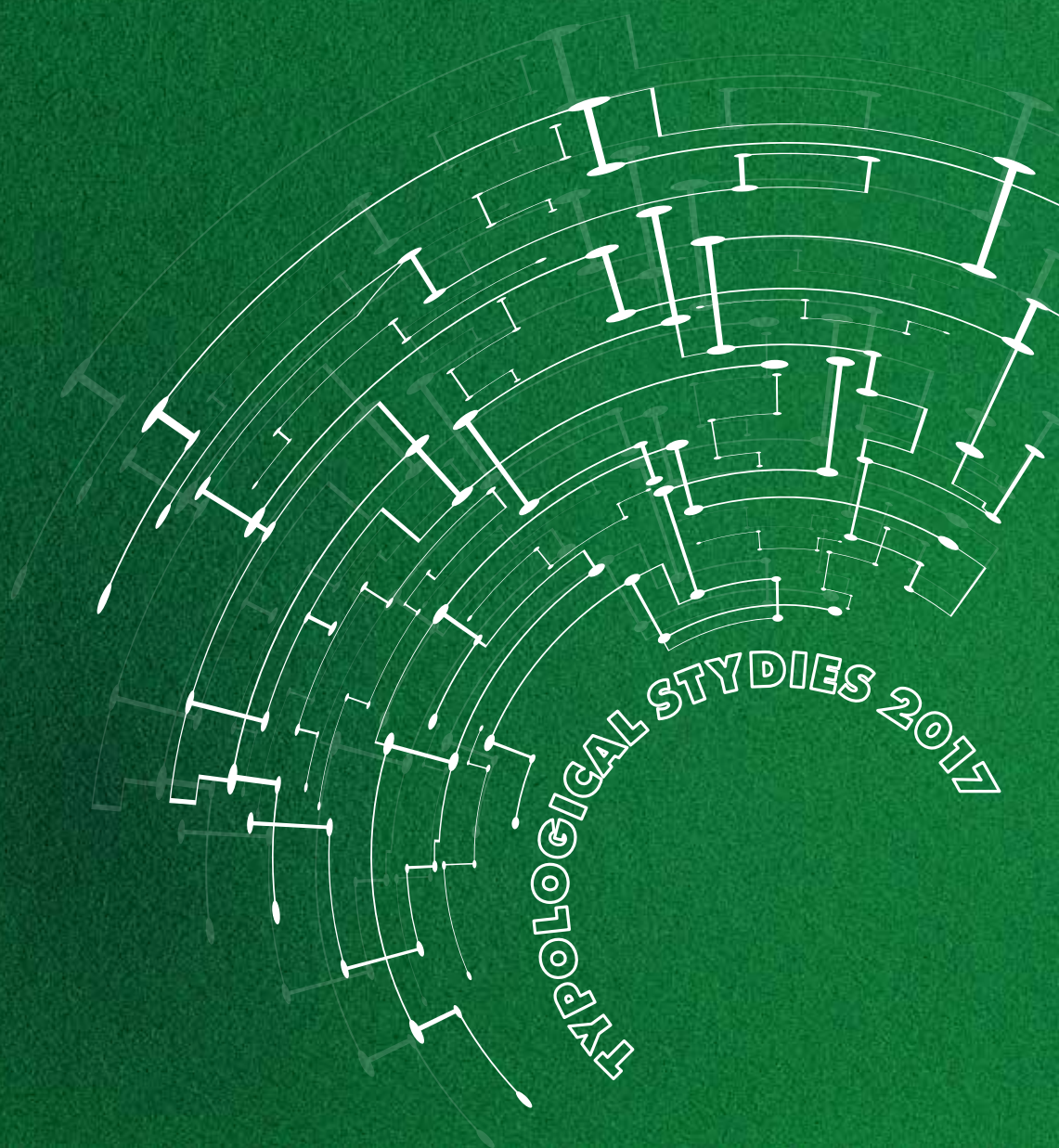
3.6.6. Use of the mining industry for terrorism financing . . . . .	137
3.6.7. Use of informal payment systems for terrorism financing . . . . .	138
<b>SECTION IV. TOOLS AND METHODS TO FINANCE TERRORISM IN UKRAINE. . . . .</b>	<b>141</b>
CONCLUSION TO THE PART II . . . . .	146
LIST OF ABBREVIATIONS . . . . .	147





# FOREWORD

---



TRIOLOGICAL STUDIES 2017

# FOREWORD OF THE HEAD OF THE STATE FINANCIAL MONITORING SERVICE OF UKRAINE MR. IGOR CHERKASKYI

---



Dear colleagues!

We are pleased to pay your attention to Typological studies of the State Financial Monitoring Service of Ukraine for 2017 within highlight the results of the work of the Financial Intelligence Unit of Ukraine and other participants of the national financial monitoring system on the exposure of modern schemes and methods used by criminals to legalize (launder) the proceeds from crime, and terrorist financing.

It should be noted that Ukraine continues to use the reinforced practical measures for the development and improvement of the national financial monitoring system in accordance with international standards.

The previous year was notable for the evaluation of Ukraine within the 5<sup>th</sup> round of Mutual Evaluation by the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.

One of the key risks that were highlighted by the experts of the Council of Europe and which, were detected in 2016 based on the results of the first National AML/CFT Risk Assessment in the area of prevention and counteraction to the legalization (laundering) of the proceeds from crime and the financing of terrorism, became the risks of widespread use of cash and terrorist financing.

Taking into account the above mentioned and other factors underlying the study of modern risks in the financial monitoring system, the SFMS generalize and publishes standard schemes of legalization of the proceeds from crime.

In addition, the need to conduct such a work is directly provided for the legislation of Ukraine and the FATF Recommendations.

In 2017, the SFMS taking into account the enhanced cooperation with MONEYVAL within the mutual evaluation, not traditionally, has conducted two typological studies instead of one.

Thus, the presented publication collected in itself typological studies of the State Financial Monitoring Service of Ukraine for the last year, which relate to:

- risks of cash use;
- risks of terrorism and separatism.

Taking into account the typologies of the recent years (Laundering the proceeds from corruption [2016], Current instruments, methods, and mechanisms of illegal funds allocation and laundering [2015], Current techniques, methods, and financial instruments of terrorism and separatism financing [2014]), we have consciously focused on the analysis of the most fundamental risks that exist today. That are the use of cash and new forms of financing terrorism and separatism.

I am convinced that typological studies prepared by the SFMS, with the participation of other state authorities and the private sector, will be useful to practitioners of the state and private sector as well as the public, who deal with the protection of the financial system from the invasions of criminals.



Igor Cherkaskyi





# PART I

## RISKS OF CASH USE

---



TRIOLOGICAL STUDIES 2017

## INTRODUCTION TO THE FIRST PART

The use of cash as the major facilitator (a tool simplifying a task at hand) within the money laundering cycle is a serious relevant issue tracked in both developed and developing countries. Cross-border cash flows have been under careful analysis of supranational institutions (FATF, Europol, European Commission, MONEYVAL, etc.) for the last decade.

Despite stable expansion of cashless payments and related technologies, the rates of cash transactions all over the world have diminished only a very little. Pan-European trends prove that the total value of Euro banknotes in circulation has been growing annually, and the above rates have been even higher than European inflation values.

Global trends provide evidence that cash (banknotes of low par value) is commonly used with payments for low-valued goods and services. In this context, a mere 1/3 of par value in circulation is spent. At the same time, there is a stable demand for high par value banknotes. With the above cash trend in mind, the latter banknotes are not used for daily payments spent on common goods and services. The anomalies detected can be directly related to illicit activities of organized criminal groups.

One of the most important preliminary conclusions related to supranational cash use analysis would lie in the claim that there is substantial lack of information regarding the use of cash for reaching both legal and illicit goals.

The use of cash remains the basic reason for suspicions regarding financial transactions implemented within financial and economic systems of both EU member-states and Ukraine.

Another aspect which is worth mentioning states that despite the fact that not all the cash transactions are a matter of crime, all the players involved in socially dangerous illicit activities (criminal actors) use cash at a certain stage of money laundering.

Despite the fluency of methods, techniques and applications of illicit activities (specifically, ever-rising occurrence of cybercrimes, virtual currency, internet scam, illegal web stores, etc.), countermeasures aimed at prevention of money laundering activities remain traditional, with cash as one of the most popular tools in money laundering for practically all types of crime.

Movement of cash via freight transports or postal services is still a blind area, and cross-border movement of other highly valuable liquid proceeds (cash equivalents by liquidity level) such as gold, diamonds, jewellery is not covered with proper attention by either EU or Ukrainian institutions. The above mainstreams vulnerabilities as generators of additional risks at both national and supranational levels.

The answer to the question regarding the reasons of active demand for cash in the money laundering process lies in the field of common specifications of tools used for this purpose, namely, for:

- need to hide a source and real holder of illicit proceeds;
- need to keep direct or indirect control over illicit proceeds;

- need to change forms of illicit proceeds to decrease the substantial volume of illicit cash and/or eliminate any possible relations to committed predicate offences.

Cash meets all the aforementioned needs since it belongs to negotiable bearer tools: it belongs to a person/entity that holds it at a specific moment of time.

Within this context, there is yet another important focus field for supranational analysis of cash flows including two approaches to financial monitoring analysis:

- cash being laundered;
- cash being used as a tool to launder illicit proceeds or financing of terrorism.

Cash has been a generator of a fundamental dilemma for criminal actors because, on the one hand, it is a goal a crime is committed for, while on the other hand, holders of such proceeds try disposing of them by converting to other forms of income for laundering.

The ratio between the monetary value of the total cash volume and the national GDP value is an important object for cash flow analysis used by leading central world banks. Absolute and relative characteristics of volume dynamics for banknotes of related par value are no less important, though.

Research of a part of counterfeit banknotes of related par values is but another important object for cash flow analysis.

Tracking international trends in identification (mapping) of countries of destination and origin for cross-border movements (including smuggling) of cash plays an important role in mainstreaming risk profiles of countries and territories.

As of today, Europol identifies Switzerland as the most important country that can be primarily vulnerable to incoming cash flows, particularly from third-world countries.

China is defined as the most popular destination country for cash movements from EU member states.

Turkey is declared the country playing an important role in transit cash movements from Europe to Middle East countries.

Nigeria is identified as the major country of origin for suspicious cash flows to EU countries.

Ukraine is positioned as a country which cash couriers declare their cash amounts imported to EU countries openly and in full. At the same time, the competent bodies of the EU countries have suspicions of legality of origin for cash vastly transported by Ukrainians through the borders of EU member states<sup>1</sup>.

---

<sup>1</sup> Why is cash still king? A Strategic report on the use of cash by criminal groups as a facilitator for money laundering. – European Police Office (EUROPOL Financial Intelligence Groupe), 2015. Web resource. Resource access mode: [www.europol.europa.eu](http://www.europol.europa.eu)



In support of the above Europol's conclusions, it is worth mentioning that according to the data from the Tax Justice Network, the total amount of USD 167 billion was illegally moved out from Ukraine in 1991-2010 (USD 16.7 billion was moved out annually on average)<sup>2</sup>.

More recent assessments implemented by the Global Financial Integrity organization demonstrate that Ukraine took the 14th place in the world among the countries with the biggest illicit flows of national proceeds moved abroad in 2004-2013 with annual rates of approximately USD 11.676 billion<sup>3</sup>.

In 2011, SFMS published a unique typology study titled "Typologies of money laundering with the use of cash".

Another typology study of 2015 titled "Standard tools, methods and mechanism for placement and money laundering" contained standard schemes of money laundering within the state and commercial sectors of economy involving financial and non-financial intermediaries with specific focus on cash transactions.

Jointly with the OSCE Project Coordinator in Ukraine, SFMS implemented the "Enhancing Ukraine's financial monitoring capacity" Technical Assistance Project. The latter involved the development of NRA.

The first NRA results presented in December 2016 prove, among other things, the following relevant risks out of 37 identified ones for Ukraine:

- low level of public and legal entities' trust to the national financial system;
- high cash circulation rates;
- high financial capital outflow rates;
- increased organized crime rates;
- non-transparent financing of political parties;
- inappropriate detection and authorization of suspicious financial transactions (including cash transactions) carried out by national PEP's.

The aforementioned risks are demand generators for both cash and money laundering transactions in Ukraine, the sources of which are unknown or illicit<sup>4</sup>. Recent events proved a necessity in mainstreaming a study regarding detection of money laundering schemes with the use of cash.

Since the financial system in Ukraine is focused on cash transactions, it is essential to pay proper attention to cash flow in particular. It is worth mentioning that the lack of public trust towards the financial system and state authorities in Ukraine complicates and impedes not only generation of sufficient resource capacity by the financial system but also its transformation into investment-related economic resources while stimulating increased cash volumes, which is high risky from the financial monitoring point of view.

2 Capital Flight from Developing Countries: Top 20 Losers [Web resource] / Tax Justice Network. – Access mode: [http://static.guim.co.uk/sys-images/Observer/Pix/pictures/2012/07/22/gu\\_wealth-offshore-02.jpg](http://static.guim.co.uk/sys-images/Observer/Pix/pictures/2012/07/22/gu_wealth-offshore-02.jpg)

3 Illicit Financial Flows from Developing Countries: 2004–2013 [web resource] // Global Financial Integrity. – Access mode : <http://www.gfintegrity.org/report/illicit-financial-flows-fromdeveloping-countries-2004–2013>

4 NRA Report [Electronic resource]. – K., 2016. – 208 c. – C. 42. Access mode (available in Ukrainian): [http://www.sdfm.gov.ua/articles.php?cat\\_id=581&lang=en](http://www.sdfm.gov.ua/articles.php?cat_id=581&lang=en)

Hence, cash is the major financial tool in financing of terrorism with such specific risks as volunteer handover of personal cash by individuals to representatives of terrorist and/or separatist organizations, deposits of proceeds to card accounts held by terrorist groups members, which are further converted to cash, cash couriers and persons implementing cash imports for persons directly involved in terrorist activities, international payment systems and electronic wallets that are very easy to use and convert proceeds to cash.

At the same time, cash remains the “most favourite” tool in corruption-related schemes. For instance, the one of the most common methods to launder corruption-related proceeds is deposit of cash to accounts held by individuals on top positions at state enterprises, institutions and organizations or related individuals and legal entities with further purchase of assets and services or investments into legal entities’ activities under their control, or allocation of cash to deposit accounts and for its further investment, as described above.

Illicit monetary asset cashing is one of the most common ways of illicit business, an activity implemented by so called “conversion centres”. Such firms are characterized by their shell attributes, they are registered under assumed names, they don’t report to tax bodies and provide cash conversion services for a certain fee. They mostly relate to groups of persons with significant experience in this activity and closely related to credit and financing institutions. Such a mechanism guarantees safe implementation of schemes for further money laundering.

In order to stop illicit business activities in Ukraine today, state authorities and law enforcement agencies are focused on fighting against conversion centres as much as possible.

SFMS has been tracking trends in the field of money laundering with the use of cash on the constant basis as well as recent risks and factors facilitating cashless-to-cash conversions.

This study mainstreams and generalizes most common schemes of the legalization (laundering) of the proceeds from crime with the use of cash and is focused on detection of the above schemes by financial intermediaries, state authorities and law enforcement agencies.



# **SECTION I**

## **USE OF CASH IN UKRAINIAN ECONOMY. GENERAL OVERVIEW**

---



**TYPOLOGICAL STUDIES 2017**



## 1.1. Overview of cash market trends in Ukrainian economy

Generally, cash within a system of economy is used in order to accommodate:

- turnover of goods, labours and services;
- transactions that are not directly related to turnover of goods, labours and services, namely those related to payments of wages, bonuses, pension payments, insurance proceeds, security payments and related payments of profits, etc.

All in all, Ukraine belongs to the group of countries with high cash flow rates in its economy while the related need therein has been formed along the whole independence of country. The state has an established and well-developed infrastructure oriented on cash and related transactions, but there is a huge gap with other world countries in terms of technologies and tools for cashless transactions.

Basic volume of cash is concentrated in large metropolises such as Kyiv, Dnipro and Odesa.

The table with graphs representing cash flow rates for different regions is demonstrated below.

### Statistics on foreign currency cash flow (depositing and withdrawal) (UAH equivalent) from the regional perspective, 2015-9 months of 2017

Region (Top 10)	2015 (UAH, million)			2016 (UAH, million)			99months of 2017 (UAH, million)			2015-9 months of 2017		
	Total	including		Total	including		Total	including		Total	including	
		DEP	WTD		DEP	WTD		DEP	WTD		DEP	WTD
Kyiv City	93 358	45 063	53 295	124 622	67 053	57 569	181 319	97 638	83 681	404 299	209 754	194 545
Dnepropetrovsk	52 614	28 985	23 629	43 399	23 596	19 803	33 715	16 059	17 656	129 728	68 640	61 088
Odesa	42 165	10 986	31 179	56 719	19 681	37 038	72 663	31 589	41 079	171 552	62 256	109 296
Kharkiv	19 594	7 427	12 167	26 156	12 197	13 959	28 458	13 161	15 297	74 208	32 785	41 423
Lviv	19 722	7 360	12 362	25 922	12 692	13 230	26 356	12 784	13 572	72 000	32 836	39 164
Zaporizhzhya	11 985	4 018	7 967	15 415	6 756	8 659	14 472	6 133	8 339	41 872	16 907	24 965
Kyiv	7 432	3 458	4 024	10 975	6 230	4 745	18 445	10 010	8 435	36 902	19 693	17 204
Pohava	8 604	3 267	5 337	11 134	5 396	5 738	12 204	5 556	6 648	31 942	14 219	17 723
Ivano-Frankivsk	8 323	2 944	5 379	11 311	5 671	5 640	-	-	-	19 634	8 615	11 019
Donetsk	8 999	2 924	6 075	13 008	5 308	7 700	12 141	4 425	7 716	34 148	12 657	21 491

DEP: Deposits WTD: Withdrawals

### Statistics on national currency cash flow (depositing and withdrawal) from the regional perspective, 2015-9 months of 2017

Region (Top 10)	2015 (UAH, million)			2016 (UAH, million)			9months of 2017 (UAH, million)			2015-9 months of 2017		
	Total	including		Total	including		Total	including		Total	including	
		DEP	WTD		DEP	WTD		DEP	WTD		DEP	WTD
Kyiv City	623 359	325 026	298 333	701 604	363 214	338 390	590 576	307 902	282 674	1 915 539	996 142	919 397
Dnepropetrovsk	259 078	119 978	139 100	271 947	130 683	141 264	217 773	107 914	109 859	748 798	358 575	390 223
Odesa	216 927	106 785	110 142	233 372	115 597	117 775	192 224	98 271	93 953	642 523	320 653	321 870
Kharkiv	190 401	104 651	85 750	219 297	117 852	101 445	193 391	103 275	90 116	603 089	325 778	277 311
Lviv	166 289	86 723	79 566	186 016	93 393	92 623	156 539	79 349	77 190	508 844	259 465	249 379
Zaporizhzhya	110 601	47 214	63 387	116 973	50 465	66 508	95 848	42 660	53 188	323 422	140 339	183 083
Kyiv	120 339	59 917	60 422	130 446	64 668	65 773	108 731	55 111	53 620	359 516	179 696	179 820
Pohava	93 632	45 571	48 061	101 563	48 774	52 789	84 561	41 505	43 056	279 756	135 850	143 906
Ivano-Frankivsk	86 482	42 082	44 400	93 400	44 636	48 764	78 424	37 502	40 922	258 306	124 220	134 086
Donetsk	84 436	41 448	42 988	94 543	45 255	49 288	79 434	38 484	40 950	258 413	125 187	133 226

DEP: Deposits WTD: Withdrawals

With its Resolution as of 11.08.2017 № 207- рш, the NBU Board approved the Concept of Cash Flow Arrangement in Ukraine. The Concept considers transfer from a partially controlled cash flow model active in Ukraine to a delegated model based on the practice when the National Bank delegates a part of its current regional functions to other market players – Cash-in-Transit banks and companies (CIT-companies), which should presumably decrease the cash flow ratio in favour of cashless transactions. The aforementioned model is applied in the United Kingdom, Brazil, the Netherlands, Finland and Sweden.

The following steps were made by NBU in the above direction in 2017:

- cash transaction threshold value for individuals was lowered to UAH 50,000 in the beginning of 2017;
- a new national cash flow strategy was approved, which presumes a transfer from a partially state controlled cash flow model yet active in Ukraine to a delegated one;
- work on a pilot project to introduce e-UAH – electronic currency to be issued by NBU was initiated.

It is worth mentioning that the high level of cash use has its negative impact on the national economy development, it weakens the latter's transparency and impedes the development of advanced technologies.

One of the factors influencing cash use rates is the high level of shadow economy.

The urgent need in drastic reforms of all the fields of Ukrainian economy as well as European and Transatlantic integration formed prerequisites for development and approval of the Comprehensive Programme of the Financial Sector Development in Ukraine till 2020 by NBU.

**Resolution of the Board of the National Bank of Ukraine as of 18.06.2015 № 391 “On approval of the Comprehensive Programme of the Financial Sector Development in Ukraine till 2020”**

Hence, in 2015, NBU defined a clear way for its policy till 2020, which will be aimed at further development of the payment market to establish a cashless economy.

One of the directions defined by the Comprehensive Programme includes facilitation to cashless payments, financial market infrastructure and oversight (the **Cashless Economy** Project) through the development of a payment infrastructure and subsequent decrease in the rates of cash flows in favour of cashless ones.

The implementation of the **Cashless Economy** Project is one of the basic strategic directions for the financial sector development in Ukraine.

Transfer of daily transactions (utility payments) and all state payments (pensions and scholarships) into cashless format is the priority task for the **Cashless Economy** Project. Up to now, there has not been a single state programme on the introduction of cashless payments in Ukraine.

In accordance with the initiated **Cashless Economy** Project, NBU cooperated with other state authorities for implementation thereof in 2017. The cooperation was specifically executed with the:

- Ministry of Economic Development and Trade in terms of introduction of mild regulation for cashless payments at each trade network participant;
- Ministry of Health in terms of its capacity to introduce cashless payments at medical facilities;
- Ministry of Culture in terms of plans for establishment of a cashless infrastructure at objects of cultural and historical heritage of Ukraine as well as during mass cultural events.

Promotion of comfortable and safe cashless payments will provide significant advantages for the state, banks, businesses as well as each and every citizen, which specifically includes:

- a capacity to boost the transformation of Ukrainian economy from an agrarian into an innovation one;
- a more transparent economy structure, increasing incoming flows to the state budget by expanding the taxation base and de-shadowing of citizens and enterprises accounts;
- an opportunity to raise revenues generated by transportation companies due to transfer to a cashless format of public transport travel costs through transparent payments (introduction of the e-ticket technology);
- increased flow of foreign tourists to Ukraine since they are used to cashless infrastructure already.

Transfer of Ukrainian economy into the cashless format may become a national-scale project aimed at reaching European welfare standards and one of qualitative change drivers in the country.



Firstly, any citizen can feel the advantage of comfortable and safe cashless payments. Secondly, this will assist Ukrainian businesses in mitigating current risks and raising competitiveness rates.

## 1.2. Use of payment cards

The use of payment cards mitigates ML/FT risks, but it does not eliminate those since it allows both cashless and cash transactions in any place of the world, even without the presence of a card holder<sup>5</sup>.

Subject to the terms and conditions of payment transactions with the use of a payment card, debit, debit-credit and credit payment schemes can be used.

The debit scheme considers a user to implement payment transactions with the use of a payment card with a specific card balance available and accounted for on his/her account.

With the debit-credit scheme, a user can implement payment transactions with the use of a payment card with a specific card balance available and accounted for on his/her account, and in case the latter is missing – through a loan (credit) provided by a specific bank.

The credit scheme considers financial transactions implemented by a user with a payment card and funds lent by a bank or under a specific credit line.

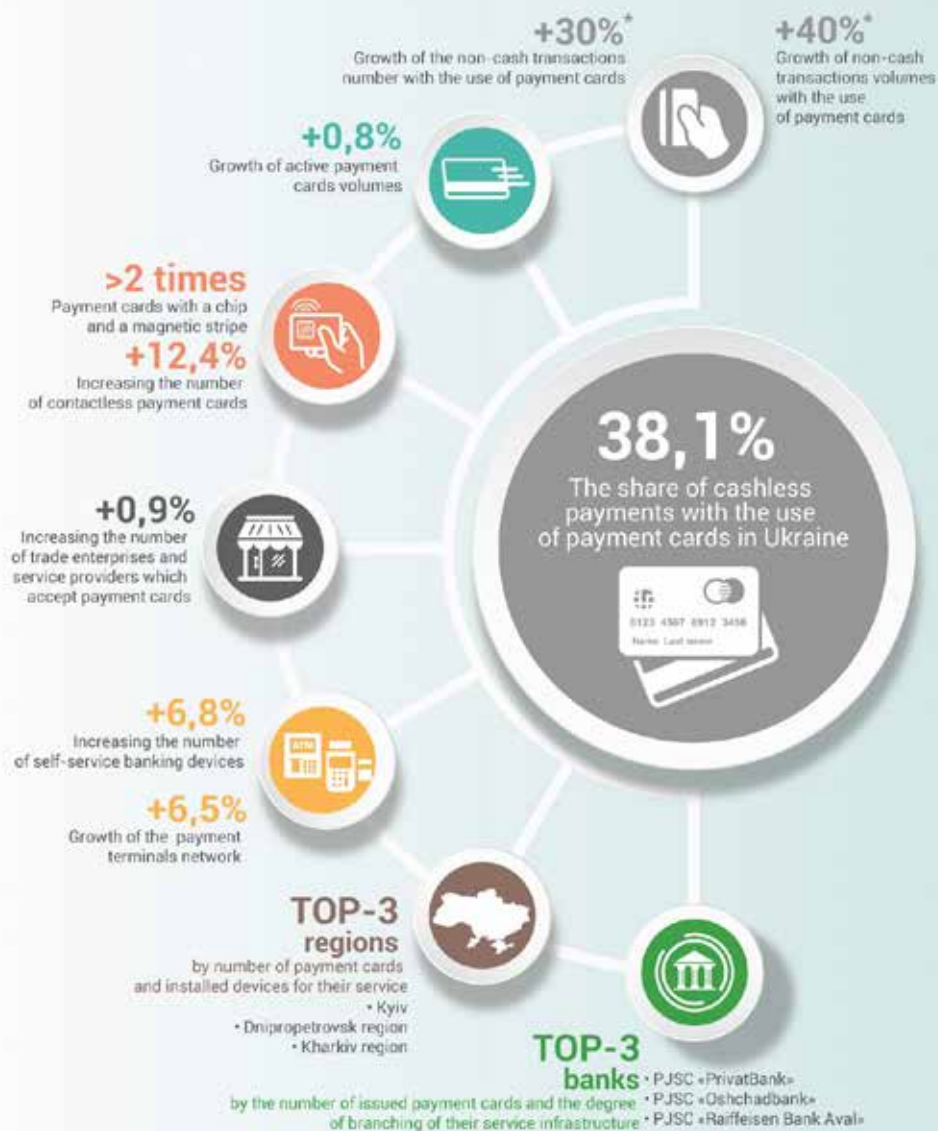
Cashless payments has become more and more popular in Ukraine.

---

<sup>5</sup> Payment card is an electronic payment tool in the format of a plastic or any other type of card issued in accordance with the valid legislation and used to initiate a transfer of funds from a payer's account or related bank account to cover the cost of goods and services, transfer of funds from personal to other person's accounts, receiving cash at bank cashier desks or ATMs as well as implementation of other transactions provided by a related contract/agreement.



# PAYMENT CARDS MARKET IN THE FIRST HALF OF 2017



For reference: as of July 1, 2017, 87 banks - members of card payment systems operated in Ukraine.

\* in comparison with the first half of 2016

### 1.3. Factors contributing to the use of cash

The basic incentive for criminals to focus on the use of cash in their illicit schemes is the lack of a possibility to define the schemes of its use, easy access to cashless-cash conversion and cash movement between participants of schemes as such.

The above transactions require no efforts from criminals in terms of extensive document management or actual provision of goods, labours or services.

In general, the factors contributing to the use of cash are consistent by their nature.

Such factors may, among other things, include the following:

- substantial share of unofficial income among both business and population, existence of a parallel – shadow economy;
- low rates of cashless payments of general public for goods, labours and services provided;
- insufficient public financial literacy;
- ease of use;
- high occurrence of USD transactions;
- lack of cash control outside the banking system;
- low general public trust towards the banking system.

This list can be supplemented with other factors such as available covert channels for movement of foreign currency abroad, positive balance of trade in foreign currency used as savings by the general public as well as shadow transactions in foreign currency implemented by both legal entities and individuals (trade in living apartments, cottages, cars, etc.).

It is worth defining the three major ways of public use of cashed foreign currency:

- building foreign currency savings that are less susceptible to inflation;
- meeting the needs of shadow trade on the national level (trade in real estate, cars, etc.);
- financing of petty traffic (shuttle trade).

Hence, the lack of Ukrainians' trust towards the financial system complicates and impedes not only savings of sufficient resource capacity by the system itself but also its transformation into economic investment resources while stimulating increased rates of cash transactions of high risk, from the financial monitoring point of view.

Increased rates of cash flows outside the banking sector in both national and foreign currencies have the following negative consequences:

- lower supply of foreign currency at the internal interbank currency exchange, which results in seriously fluctuating UAH exchange rates;
- weaker capacity to raise state foreign currency reserves, which results in lower stability of the national currency;
- significantly lower national investment and credit resources, which results in artificial demand for foreign loans while causing greater national debt and debts owed by legal entities;
- shrunk taxation base due to shadow cash flows;
- further expansion of shadow economy the above actually provides for;

- increased the source of currency outflow abroad.

In order to ensure efficient risk management for cash flows, there is a need to:

- improve public financial literacy in the field of payment card use;
- improve convenience of utility payments, fees for services provided by state authorities, taxes and other regular payments through the use of payment cards;
- expand the capacity to implement cashless payments at each and every trade facility and service provider;
- revise thresholds for cash transactions;
- improve the level of public trust towards the banking system of Ukraine;
- mitigate tax pressure on businesses;
- continue the development of mobile payments and mobile apps;
- improve safety of cashless transactions.

## 1.4. Cash transaction threshold values for inter-entity transactions

Substantial amount of circulated cash forms threats for the banking system stability, national economic security and increased development rates of shadow economy.

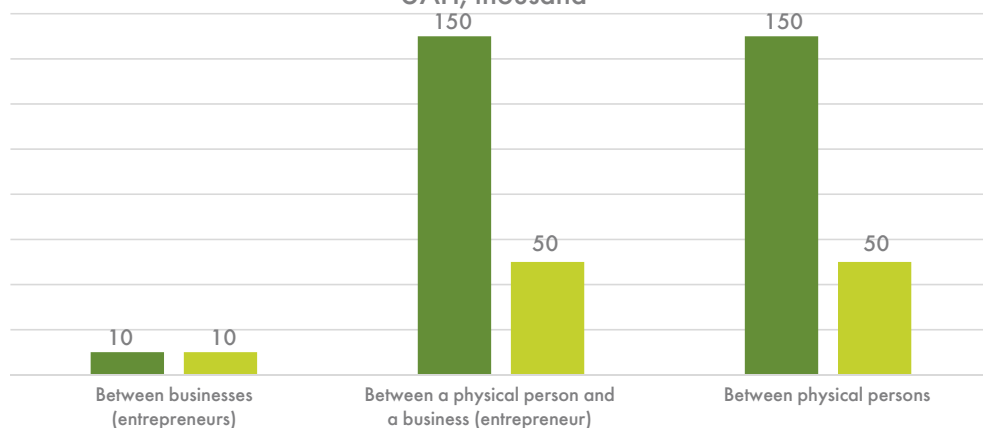
Such a trend is mostly provoked by consequences of the world financial and economic crisis and observed in a number of foreign states. In order to prevent the above as well as money laundering, cut the funds spent on cash flows, raise bank liquidity, improve control over tax proceedings, lower criminal risks in the field of regulatory practice in developed and developing countries, various restrictions on cash transactions have been getting more and more popular at the national level, including those for individuals.

Equivalent measures have been introduced in Ukraine, since 2013 NBU is setting restrictions on cash transactions for sold goods, implemented labours or provided services. In 2016, related threshold values for individuals were lowered significantly (by almost three times).

Hence, as of 2017, the value of transaction payments set for businesses (entrepreneurs) has been UAH 10,000 per day; UAH 50,000 per day – between a Individual and a business (entrepreneur); and UAH 50,000 per day – between individuals under trade agreements that require notary certification.

Payments exceeding the above threshold values to be implemented through banks or non-banking financial institutions with a license for money transfers without opening an account by transferring funds from a current account to another one; or through depositing an amount to a bank for its further transfer to current accounts.

Dynamics of ceiling values for cash transactions,  
UAH, thousand



■ Ceiling value valid since 01.09.2013 till 03.01.2017    ■ Ceiling value valid as of 04.01.2017

Restricted cash flows fully correspond to related international experience of many European countries (France, Belgium, Portugal, Italy, Spain and Greece) that set threshold values for cash transactions. Other countries also plan introducing similar norms.








At the same time, solving the issue of substantial cash transactions impeding economic development of a country nowadays and raising efficiency of the regulator's monetary policy require development of cashless retail payments as well as special payment tools for the general public.



The threshold of cash payments will be **UAH 50 000** since January 4, 2017



**Positive effects:**

-  Narrowing of the cash use area and expanding of the cashless area
-  Ensuring stability of cash inflows to the banking system and accelerating of its circulation
-  Additional resources for the economy crediting
-  Reducing of the shadow economy volumes
-  Legalization of income of the population
-  Increase transparency of financial flows and the fight against corruption
-  Reduce of the cash handling costs

**The restrictions will not affect the daily purchases of the population, since they will concern only large purchases**



**European experience:**

thresholds of cash settlements

 <b>€2 500</b>	 <b>€1 500</b>	 <b>€1 000</b>	 <b>€3 000*</b>	 <b>€1 000</b>
Spain	Greece	France	Italy	Portugal



## 1.5. Cash in money laundering

The use of cash in money laundering schemes is based on the necessity to reach certain goals for criminals:

- hide the tracks of illicit proceeds' origin;
- hide persons who earned (earn) illicit proceeds and those initiating the laundering process itself;
- ensure convenient and due access to funds gained from illicit sources;
- form conditions for safe and convenient use of illicit funds.

While analyzing the origin of out-of-bank cash flows, it can be claimed that a certain amount of cash actually does not belong to illicit activities but rather illicit cashless-to-cash conversion.

Since criminals tend to keep their proceeds liquid, cash is in fact the first stage in money laundering while preceding the state of "allocation" whereat criminals try minimizing available risks related to possible seizure of cashless funds.

Cashless flows are easier to control than cash ones. Funds transferred from one account to another one can be tracked by banking institutions, law enforcement agencies and other state authorities.

Hence, in order to implement a money laundering scheme, the so called "circuit breaking" transactions are used. The latter are applied in order to mask the tracks of illicit proceeds by changing fund holders, their physical movement and actual withdrawal in cash.

## 1.6. Cryptocurrency as a tool in money laundering

Financial intelligence units and law enforcement agencies has focused their particular attention on investigation of comprehensive money laundering schemes with the use of cryptocurrencies in the last few years. Particularly, specifics of financial investigations including the use of cryptocurrencies for money laundering have been studied<sup>6</sup>.

A speed of cryptocurrency transactions is extremely high, identification of their participants is almost impossible, especially in a non-regulated market of financial services as such, which poses one of the greatest risks. That means that money can be withdrawn or converted much faster than through more traditional channels. Such a speed of a transaction results in complicated monitoring thereof as well as additional difficulties in fund freezing.

As of late, trends on promotion of virtual currency use in illicit financial schemes aimed at the legalization of the proceeds from crime have been observed. The abovementioned proceeds are most often acquired in cash.

---

<sup>6</sup> Cryptocurrency is an equal, decentralized digital currency based on cryptography principles for verification of transactions and formation of the currency as such. It is in fact a web currency allowing anyone to own currency and use it. Such transactions are beyond recovery and cannot be blocked. Transactions implemented with the use of cryptocurrency are very difficult to track.



The fact of cryptocurrency use by organized criminal groups as a tool for illicit activities related to IT fraud technologies of so called "financial pyramids" has been widely spread.

The basic factors influencing the growth of the above trend include the lack of the legal status for virtual currencies in Ukraine, lack of both external and internal administration as well as controlling centres thereof (full decentralization renders any transaction cancellation or arrest impossible), anonymous payments, etc. Both the above factors as well as simultaneous international spread and amendment of financial legislation in specific countries to regulate relations dealing with virtual currencies make this category of financial services ever more attractive for illicit activities.

In order to detect threats emerging due to the use of virtual currencies, it is possible to define the following risk indicators used in relation to cryptocurrencies:

a virtual currency administrator or currency exchange company located in one country but having accounts in other countries where they usually have no substantial client base;

flow of funds between bank accounts maintained by various virtual currency administrators or virtual currency exchange companies located in different countries (which can prove a spatial activity since it doesn't correspond to a business model);

volume and frequency of economically irrelevant cashier transactions (sometimes structured below their reporting thresholds) implemented by a virtual currency administration or virtual currency exchange company owner.

The use of AML/CFT control tools for virtual currency transactions may be of use to prevent any violations in this field.

# SECTION II

## DETECTION OF RISKY CASH TRANSACTIONS

---



TRIOLOGICAL STUDIES 2017

International practice involves a number of external characteristics pointing at a suspicious or illicit transaction implemented by a client. Various models or algorithms are developed for their detection, and they assist in identifying a money laundering scheme.

Hence, investigation of these cases is commonly initiated with defining a client's risk profile, detecting cash transactions, their origin and further use of funds as such.

At the same time, to establish a reason for suspicion about financial transaction legality, there is an assumed need in a study of a related client, other transaction participants (past and current) as well as their particular financial and economic activities, actual financial transactions implemented under a scheme and related documentation.

It is worth mentioning the following indicators of illicit cashless-to-cash conversion schemes as well as general ML/FT schemes:

**regarding financial transaction participants:**

- registration of a company to men of straw (without a specific residence, mentally disabled, students, elderly people, foreigners, convicts, deceased or those registered under purchased, stolen or lost documents);
- a person is the sole founder, manager and accountant of the same company (sole founder and leadership staff);
- persons living in a region which is different from an entity's registration region are the founders of a company;
- persons living in the territories beyond governmental control of Ukraine or within the delimitation areas (specific districts of Donetsk and Lugansk oblasts) are the founders of a company;
- persons registered or crossing the border of Ukraine for the countries under targeted financial sanctions;
- frequent changes in founders, owners or leadership of an economic entity, impossibility to locate the leadership (manager/director, chief accountant, etc.);
- low authorized capital;
- names of economic entities are often similar to names of state enterprises or well-known brands;
- lack of any indicator for authorized activities or minimum authorized activity rates;
- lack of staff, production or warehousing premises for the implementation of authorized activities;
- offices of economic entities are registered at the place of mass registration of entities as such;
- matching registration addresses of transaction participants;
- newly established economic entities (so called "day-flies", "holes" or "butterflies" that usually exist for a certain taxation period, which complicates control over their activities);
- economic entities submit their tax reporting with minimum income or substantial income but low tax paid;

**regarding financial and economic activity of financial transaction participants:**

- daily cash flow is usually increased in the end of the week, the amount on a related account has no funds left every next evening or morning, or the above amount is significantly lower;

- available substantial number of signed similar standard agreements, cost estimates, acceptance acts related to implementation of labours or provision of services, etc.;
- use of multilateral transactions and payments with a high number of participants for the above transactions located in different territorial areas or registered at the same address;
- no cash flow on banking accounts held by economic entities or extremely low level of financial transactions of a recently established company;
- wide range of counteragents transferring funds to their accounts with various payment details;

**regarding content of financial transactions:**

- confusing or unusual nature of a commercial agreement (transaction), which is economically irrelevant or has no obvious legal purpose;
- non-conformity of an agreement (transaction) with activities of an economic entity provided by statutory documents;
- multiple transactions or agreements that can be presumed as the way to evade mandatory controlling procedures provided in the current legislation;
- substantial amount of cash earned from commercial activities that cannot be characterized by intense cash transactions;
- an agreement does not provide any notion on penalties to be paid by counteragents for non-abiding with payment terms or delivery terms for goods, neither there is any notion of their duty assurance;
- a significant number of financial transactions implemented by a person/entity with accounts of other persons/entities based on a power of attorney provided that account holders had no personal contacts with bank employees for a long time or as of the moment their accounts were opened;
- deposits of funds from several economic entities during a single banking day to a client account that are converted to cash the same day or transferred to another account, which results in no funds remaining on the account in the end of the banking day, or their amount is significantly lower;
- a legal entity or an individual-entrepreneur implements account transactions dealing with trade in goods, payments for labours or services without any other payments under the same account, including mandatory payments and budgetary fees;
- transactions with securities with the aim for the clients to acquire cash;
- significantly increased amount of funds at a person's/entity's account, which is not related to a person's/entity's activity, that is further transferred to a counteragent in another bank or used to procure bearer securities;
- a substantial amount of cash deposited by a person who cannot afford such transactions under his/her income level;
- payment of penalty (charge, fine) for non-fulfilment of a product supply (labour fulfilment, service provision) agreement or breach of the above agreement in case the amount of the penalty exceeds 10% of the total amount for non-supplied goods (non-fulfilled labours or non-provided services);
- obvious non-conformity of incoming/outgoing payment details (e. g., funds incoming as a payment for goods, labours and services in full are spent on procurement of securities or agricultural products);



- financial transactions related to trade in goods (payment for services), with their value difficult or impossible to define (i. e., intellectual property; specific types of services with no constant market value);
- non-conformity of the value of goods or services provided in a contract with their market value;
- regular financial transactions related to bill business implemented by a person/entity in case the latter is not the issuer or receiver of funds under the above bills and has no license of a securities professional;
- debit transfers of cash from a legal entity's account, which is not related to the type of its authorized activities;
- amounts of financial transactions implemented by a client don't conform to his/her property (financial) situation;
- closing of accounts held by a scheme participants after a certain cycle of cash transactions or drastic cancellation of the above transactions under the above accounts.

A number of Cases related to money laundering with the use of cash transactions as a "circuit breaker" method for financial transactions and masking the origin of the above funds are provided below.

### Case 2.1. Money laundering implemented by individuals while involving a non-resident company

In accordance with the information received from foreign FIUs, SFMS has implemented an analysis to detect a scheme of financial transactions that can be related to money laundering.

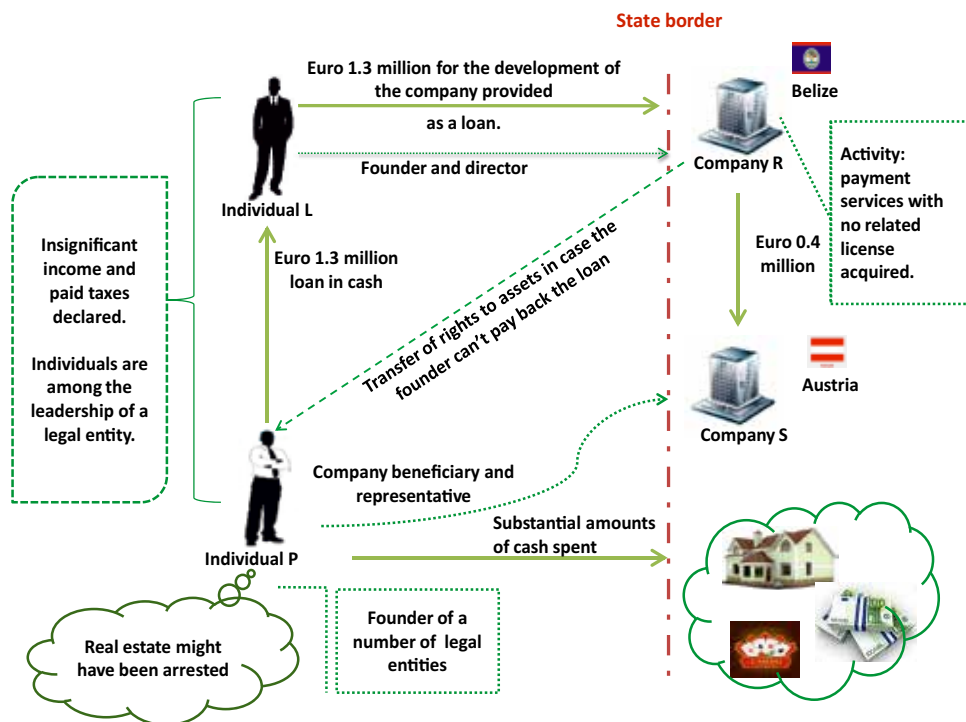
It is known that the **Individual P** transferred funds to the **Individual L** in the amount of **Euro 1.3 million** for the development of the **Non-Resident Company R**. The above funds, which are considered suspicious since the **Individual P** only declared an insubstantial amount of funds, have been transferred for the benefit of the **Company R**. In case the loan acquired by the **Individual L** is not paid back, 100% of the **Company R's assets** shall be handed into the ownership of the **Individual P**.

It is known that the **Non-Resident Company R** implemented transactions in the amount of **Euro 0.3 million** for the benefit of the **Non-Resident Company S** a beneficial owner of which is the **Individual P**. Moreover, the **Individual P** is the founder of a number of legal entities, with the **Individual L** registered as the director of one of the above entities.

It is worth mentioning that the **Individual P** spends a substantial amount of money outside Ukraine as hotel fees, at casinos and as cash withdrawals.

Hence, there are reasons to suspect the **Individual P** and **Individual L** of joint activities in laundering of non-declared proceeds of suspicious origin.

An investigation is being conducted by a law enforcement agency.







# SECTION III

## INTERNATIONAL MONEY LAUNDERING PLATFORMS

---



TECHNOLOGICAL STUDIES 2017

Globalization of the world's financial system is closely related to rapid growth in capital movement rates. Deregulation and liberalization of financial markets have resulted in a certain globalization of the money laundering process.

In order to mask illicit activities, so called "platforms" or professional networks are established. They are commonly located outside a country of origin and hence might not be covered by the national AML/CFT legislation.

### **Case 3.1. Cross-border money laundering network**

---

There has been detected a group of non-resident companies with their activities aimed at accumulation and allocation of money transfers acquired under a wide range of details both in Ukraine and abroad. All the companies were registered in several countries under the same "virtual" mass registration addresses. Each of the above companies' authorized funds constituted approximately USD 1,000. The above companies were registered by mostly the same persons. Their secretaries, directors and forged owners were represented by mostly the same companies. Persons authorized to manage accounts of the above companies were resident individuals of the same country related to each other. The above proves the existence of a group providing money laundering services through the "established" professional network while using the services of professional company registration and incorporation agents, lawyers and accountants.

During the related investigation, it was detected that funds were transferred through dozens of the same companies.

It was also revealed that the above non-resident companies had accounts opened at an EU banking institution but registered at offshore jurisdictions.

The persons authorized to manage accounts of the above foreign companies were citizens of Ukraine suspected of money laundering, including that through a professional money laundering network in Ukraine through so called "conversion centres".

Further investigation revealed that the aforementioned "conversion centres" involved companies with their accounts opened in the same Ukrainian banking institution.

Analysis of founding connections of the above banking institution revealed that the same individual was the ultimate beneficiary both in Ukraine and abroad.

As of now, the related Ukrainian bank's license has been withdrawn, and the bank itself has been liquidated due to suspicions of money laundering.

Apart from the evidence listed above, structured payments and carousel schemes for the implementation thereof at Ukrainian and European banks as well as involvement of the ever-growing number of "service users" are yet another proof of the professional approach to money laundering services.

At the inception stage, money transfers were executed in equal substantial amounts (more than USD 10 million). Next, the number of companies was multiplied several times, and money transfers were executed for both substantial (more than USD 10 million) and insubstantial amounts (from USD 1 million to USD 10 million) in accordance with a carousel scheme, which results in impeded detection of a clear route of funds moved from companies which transferred them to end receivers.

In specific cases, a substantial number of daily transactions was observed (commonly, from 10 to 30 incoming and outgoing money transfers were implemented under the accounts daily) in both

substantial and insubstantial amounts with the positive balance in the amount from USD 1 million to USD 5 million in the beginning of every banking day, which formed Brownian movement of funds. It is extremely complicated to define the actual source of funds and their further movement at this stage.

Incoming transactions included both transfers from presumably shell non-resident companies and those from the real sector (specifically those registered in Ukraine), conversion centre members and those companies that were active at different stages of money transfers.

A substantial number of Ukrainian citizens as well as persons from other countries fluent in Russian (Russia, Armenia and Azerbaijan) stand as authorized persons and beneficial owners of the companies transferring funds for the benefit of the aforementioned companies.

Analysis of network companies IP address used as remote access points to related bank accounts proves that control over the money transfer process was implemented from a single centre located in Ukraine. The same IP addresses were used for simultaneous access to both Ukrainian and foreign accounts.

Moreover, a number of non-resident companies presumably registered by their virtual addresses (mass registration address for companies) were detected. These companies had their email addresses and accounts opened at foreign banks. They also operated in accordance with a different principle.

The above companies, other non-resident companies and Ukrainian companies executed a number of transfers under the chain in substantial amount (more than USD 1 billion). The above funds (including those coming from Ukraine) had been preliminarily received at Ukrainian accounts of 3 individuals and were detailed as "security fees, treasury bill fees and investment certificate fees".

The aforementioned individuals further withdrew a part of funds from related accounts in cash, and the rest was re-deposited to the accounts and transferred abroad again detailed as "treasury bill fees". This is how a carousel scheme was used to launder proceeds previously moved out of Ukraine.

The same individuals were authorized to manage related companies' accounts and their beneficial owners at the same time.

Accounts of individuals and Ukrainian companies were opened at the same Ukrainian bank mentioned above. The ultimate beneficial owner of that banking institution was the individual owning the above foreign bank hosting accounts for non-resident companies participating in this scheme.

Therefore, transactions executed both in Ukraine and abroad are related and implemented through a "cross-border money laundering network" using both Ukrainian and foreign centres and focused on meeting the needs of both national and foreign "service users".

**There are the following basic indicators of international money laundering networks:**

- different geographical location of companies, banking institutions hosting their accounts, leadership/companies, authorized persons and beneficial owners, generic IP addresses used for remote access to account management;
- the same network member companies are used at various stages of the money laundering;
- network member companies are registered in countries with simplified registration procedures such as Panama, the United Kingdom, the Seychelles, Belize, Cyprus, etc.;
- member companies are registered under the same or several virtual addresses or email addresses with the assistance provided by third parties (advocates, lawyers, etc.);
- directors/secretaries/false owners are claimed as the same companies controlled by the above service providers and are directors/secretaries of a number of other companies at the same time;

- bank accounts of the companies are opened at one or several related banking institutions and in countries with lowest commission rates for financial transactions in order to minimize expenditures for bulk of “false” transit transactions;
- in many cases, accounts are opened through bank “representation” located in other countries, which allows authorized persons opening accounts without even visiting the country that hosts it;
- the same persons are beneficial owners of banking institutions related to the networks;
- citizens of a single or several countries similar by their cultural/language/economic relations are authorized persons and beneficial owners of all the member companies;
- accounts are opened at banks providing remote access services for web-based financial transaction management;
- control over financial transactions at accounts owned by member companies is implemented from the same IP addresses;
- “black”, “grey” and “white” flows of funds are mixed at numerous stages in order to hide the origin of the above funds and their further movement;
- accounts mostly host transit transactions;
- monthly turnover of member companies might be as high as hundreds of USD millions;
- structured incoming and outgoing transfers – equal transfer amounts, substantial amounts in cash.

The issues occurring during the investigations into international networks might include the following:

- difficulties in distinguishing “black”, “grey” and “white” flows to detect the origin of funds at accounts as well as their further specific movement;
- restrictions set by national legislations resulting in barriers while acquiring required information;
- detection of actual controllers/beneficial owners due to an opportunity to register companies for men of straw/false companies;
- international networks are based on (and related to each other) financial institutions operating in different countries.

**Solutions:**

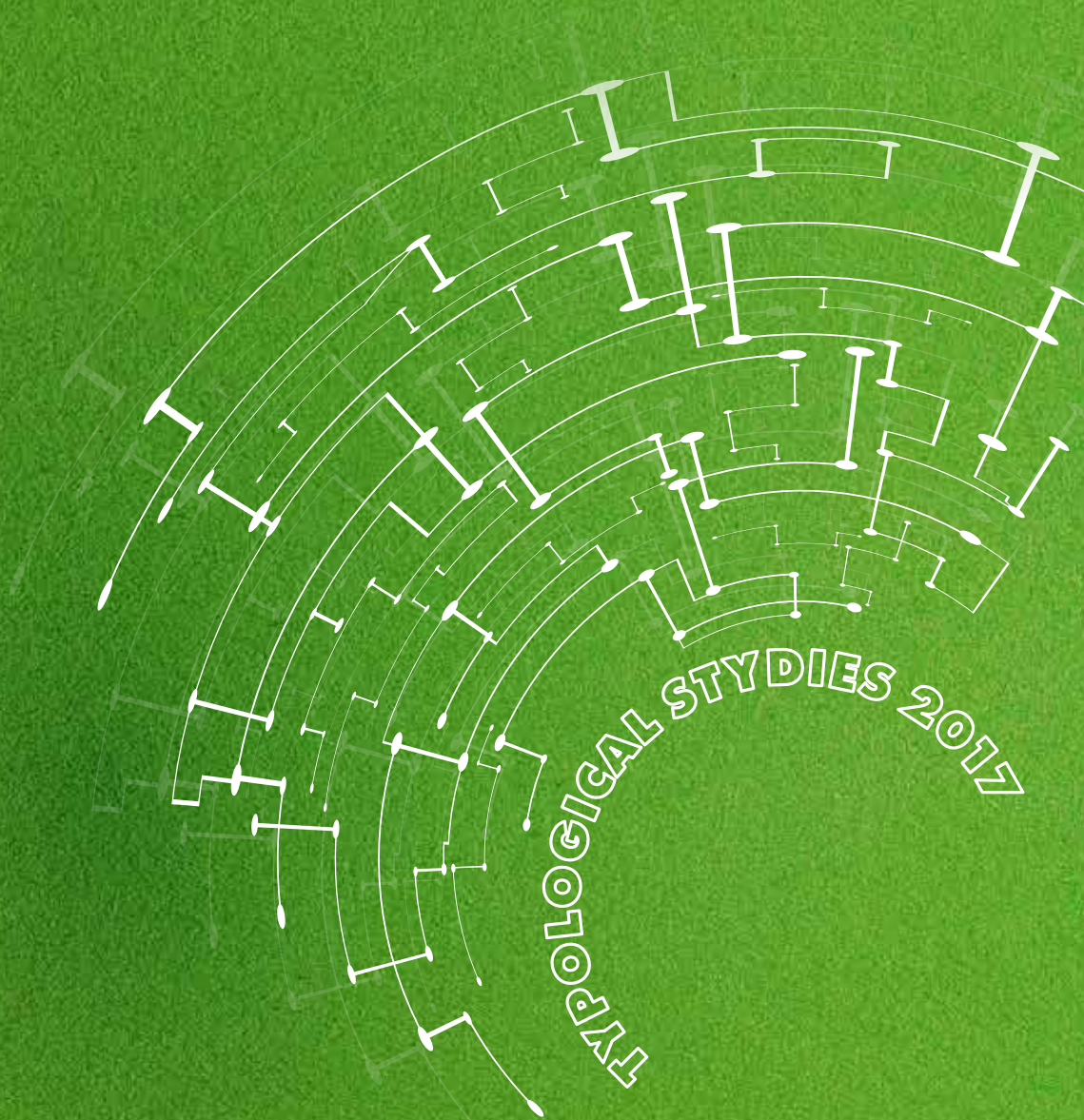
- arrangement of efficient international cooperation;
- political will of member countries;
- implementation of international analytical studies and development of related counteraction strategies;
- establishment of joint working groups;
- legal improvements to remove existing barriers for related information exchange;
- maintenance of electronic registries of actual beneficial owners of a company;
- improvement of transparency for financial systems at both the national and international levels.



# **SECTION IV**

## **CONVERSION CENTRES AND THEIR OPERATIONS**

---



TECHNOLOGICAL STUDIES 2017

As of now, illicit mechanisms in this field have been significantly evolving due to constant legal amendments, strengthened control implemented by state regulators over banking and non-banking financing institutions and state policy aimed at elimination of shadow economic schemes (in the first place, so called “conversion centres”).

It is worth mentioning that the corruption component is the main one in the operation of conversion centres since it facilitates specific persons (groups of persons) who are public officials or leadership of commercial structures, including professional financial market participants, to gain loyalty of a specific banking facility’s leadership.

The emerging need in substantial amounts of cash flowing outside of the banking system resulted in the establishment of various schemes and structures for acquisition thereof (use of shell companies, men of straw, forged documentation, etc.).

High demand for currency conversion services (cashless form-cash or vice versa – cash-cashless form) is also caused by the rates of economy criminalization. The criminal economy sector requires cash for direct illicit economic activities, including bribes and accumulation of illicit profits.

The schemes used by offenders to withdraw funds from the real sector of economy to conversion centres are diverse. Those can be tools for tax loans provided through sales of actual goods for cash not registered by any accounting procedures, schemes applying various “garbage” securities, “pseudo-insurance” services, agreements under fake commitments for further cash withdrawals from a bank cashier desk, etc.

At the same time, the above schemes and mechanisms are actively used for theft and misappropriation of funds held by state enterprises, facilities and organizations, including those during tendered procurements. Beneficiary companies use the so called “conversion centres” for converting their proceeds to cash to form required amounts for “kickbacks” proposed to their customers’ leadership, legalize overstated value of goods, labours and services, forge financial and economic documents required to obtain budgetary allocations for their further use in the interests of related stakeholders.

Money laundering schemes with the use of cash are commonly rather complicated and confusing. Cashless-cash flows provide for presumably shell economic entities and men of straw.

Involvement of third parties in money laundering schemes with the use of cash is used to avoid suspicions regarding the customers of cash and discharge them from any criminal liability.

Operations of conversion centres provide constant income for their founders; hence, they are quite a popular type of illicit business to cover the needs of economic entities and organized crime. Such illicit operations as well as establishment of conversion centres are often implemented under direct facilitation, assistance or even participation of employees of financial institutions, including bank workers, lawyers, advocates, notaries, auditors, etc.

In terms of practical concerns to detect professionals involved in money laundering or conversion centre operations, SFMS received information from law enforcement authorities regarding the results of consideration of case referrals (additional case referrals) demonstrating **2,194** criminal



proceedings ongoing in relation to conversion centre operations only for the period from 2013 till the first 9 months of 2017.

Considering the facts mentioned in the above materials and in accordance with Article 205 of the Criminal Code of Ukraine "Fictitious entrepreneurship", law enforcement authorities implement 413 criminal proceedings related to the establishment or procurement of economic agents (legal entities) in order to hide illicit activities or implementation of prohibited activities. This specifically includes 108 proceedings in 2013, 79 proceedings in 2014, 79 proceedings in 2015, 74 proceedings in 2016 and 73 proceedings in the first 9 months of 2017.

In order to legalize illicit proceeds, individuals and legal entities use the following basic tools for this type of criminal activity:

- involving men of straw and shell companies, including newly established legal structures with a sole founder and leadership;
- fake agreements, forged documentation;
- use of non-return financial support;
- cashless-cash conversions through accounts held by legal entities and individuals with the use of various banking institutions.

Below goes a number of schemes related to money laundering with the use of cash transactions as "circuit breakers" and tools to mask the origin of related proceeds.

### Case 4.1. Cashless-to-cash conversions

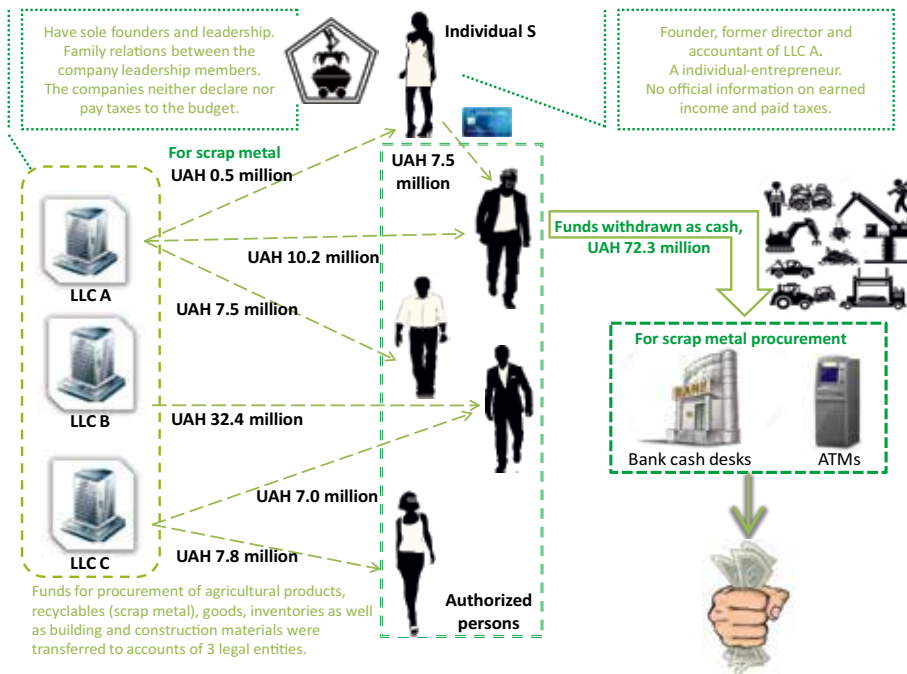
In accordance with an analysis implemented, SFMS has discovered a cashless-to-cash conversion scheme using a group of legal entities and related individuals.

Funds from a number of legal entities with different details were received to accounts of **3 legal entities**. The details for the above transfers specifically included payments for agricultural products, recyclables (scrap metal), goods, inventories as well as building and construction materials. The funds were further accumulated at current and card accounts and withdrawn in cash by authorized persons through bank cashier desks and an ATM network. The total amount of funds converted to cash for scrap metal procurement constituted **UAH 72.3 million**.

The majority of the aforementioned legal entities are newly established and having sole founder and leadership. The companies involved in the scheme don't have any declared income or taxes paid.

Authorized persons are family related, and some of them acquired substantial amounts of funds simultaneously from a sole company involved in the scheme. The above funds were further converted to cash.

An investigation is being conducted by a law enforcement authority.



### Case 4.2. Cashless-to-cash conversions

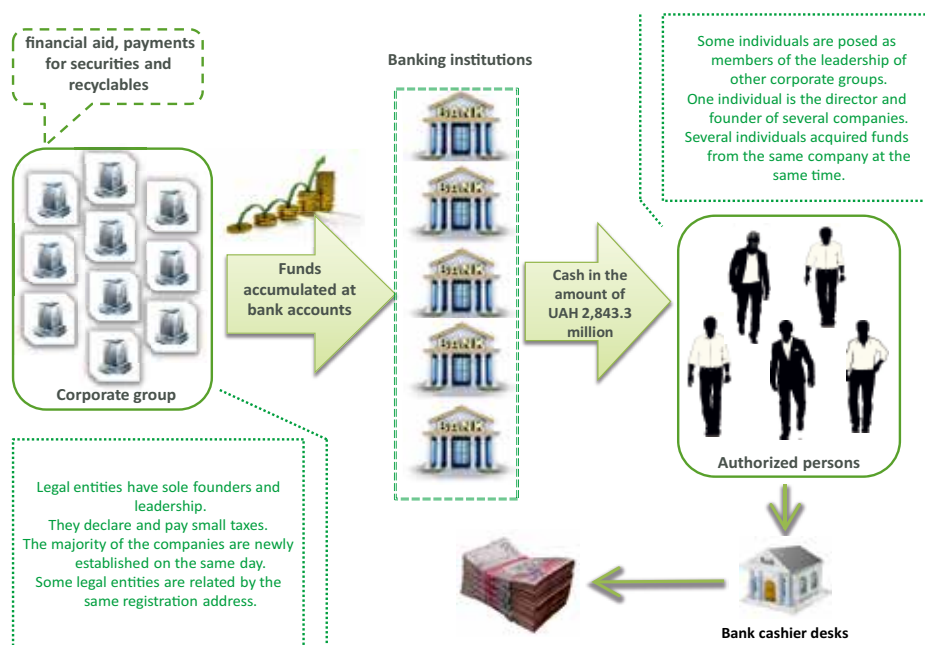
In accordance with an analysis implemented, SFMS has discovered a professional money laundering scheme with the use of a conversion centre.

It has been established that funds from various legal entities were transferred to accounts of **10 legal entities** as financial support, payments for recyclables and securities. The above funds were further accumulated at the bank accounts of the aforementioned companies and withdrawn in cash by authorized persons through bank cashier desks for the procurement of goods. The total amount of funds converted to cash constituted **UAH 2,843,300 million**.

The majority of the aforementioned legal entities have sole founders and leadership, with the most of those being newly established and registered on a single day. Some of them have the same address of registration. The above companies pay minimum taxes while having substantial amounts of declared gross income.

A peculiar fact is that the aforementioned authorized persons are also founders, directors and/or accountants of a group of other companies. Some of the above individuals acquired substantial amounts of funds simultaneously from a sole company involved in the scheme. The above funds were further withdrawn in cash. One of the above individuals is the director and founder of two of the aforementioned companies.

A law enforcement agency is in the middle of a related investigation.



### Case 4.3. Cashless-to-cash asset conversions

In accordance with an analysis implemented, SFMS has discovered a cashless-to-cash conversion scheme for substantial amounts of proceeds.

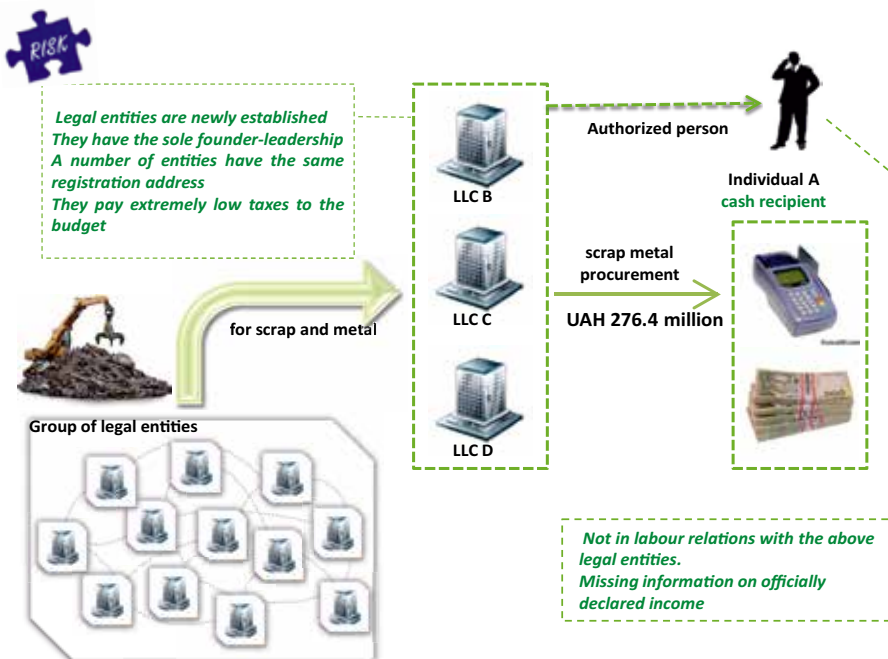
A group of legal entities has been accumulating cashless funds at their accounts previously received from a number of legal entities mostly detailed as payments for scrap or metal. The bigger share of the above funds was later withdrawn by the authorized **Individual A** through bank cashier desks and POS terminals. Cash withdrawals were implemented on the same day the funds were received at the aforementioned accounts.

The total amount of cash withdrawn by a group of legal entities with the use of the **Individual A** constitutes **UAH 276.4 million**.

The aforementioned legal entities are newly established and have sole founders-leadership. Some of the above entities have the same registration address and pay minor taxes.

The authorized person is not in labour relations with the above entities, and there is no information on his/her officially declared income.

A law enforcement agency is in the middle of a related investigation.



### Case 4.4. Cashless-to-cash asset conversions

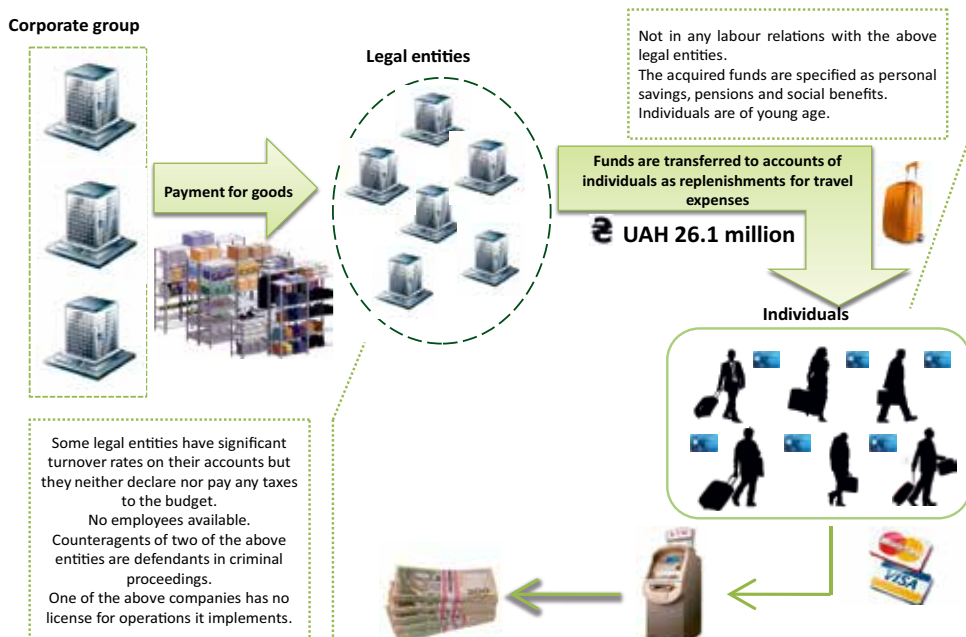
In accordance with an analysis implemented, SFMS has discovered a cashless-to-cash conversion scheme with the use of a group of legal entities and individuals.

Funds from various legal entities were transferred to accounts of **6 legal entities** as payments for goods. The above funds were later transferred to card accounts held by individuals detailed as “travels and accommodations”. The funds were further withdrawn by individuals in cash through an ATM network and bank cashier desks. The total amount of funds converted to cash constitutes **UAH 26.1 million**.

The most of the above legal entities have substantial turnover rates on their accounts but have no employees. Neither do they declare or pay any taxes to the budget. Counteragents of two of the above entities are defendants in criminal proceedings.

Individuals-recipients of the above funds at their card accounts are mostly young and not in any labour relations with the above legal entities. They only acquire social benefits from the state.

A law enforcement agency is in the middle of a related investigation.



**Case 4.5. Cashless-to-cash asset conversions**

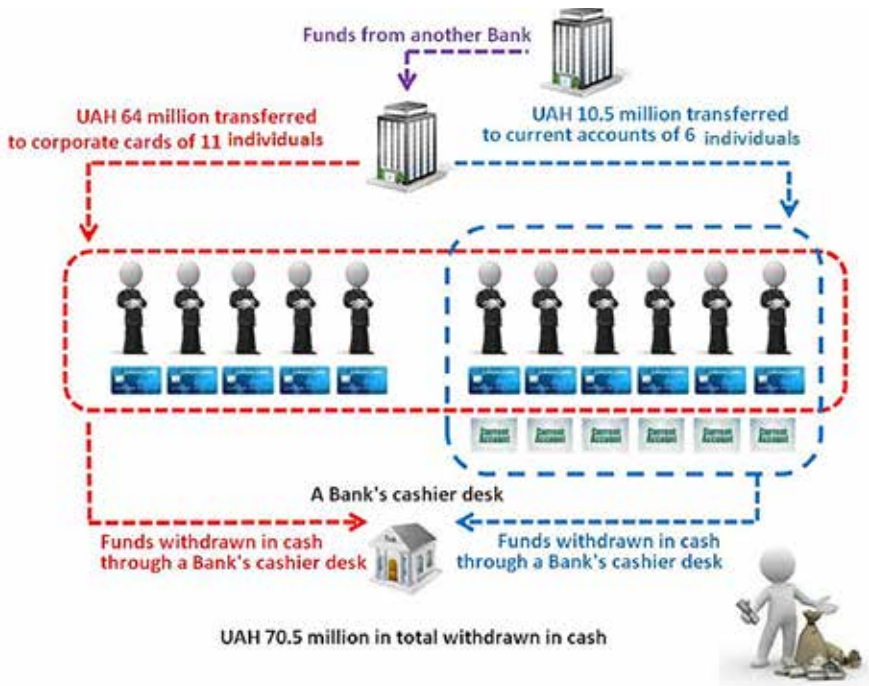
A legal entity receives funds at its current account from its current account in another bank detailed as "money transfer to a personal account".

The above legal entity transfers funds in the amount of **UAH 64.0 million** detailed as "financial aid" for the benefit of **11 individuals** who are employed by the above legal entity. All **11 individuals** have corporate cards, and 6 of them have additional current accounts.

All cashless funds are transferred to corporate cards and later converted to cash.

After a related banking institution had inquired the details of the above transactions, the above legal entity stopped all the suspicious financial transactions through the banking institution.

A law enforcement agency is in the middle of a related investigation.





#### Case 4.6. Use of a presumably shell company

SFMS has acquired information from a law enforcement agency on a discovered money laundering scheme based on tax evasion committed by companies operating in the real economy sector.

The **Individual A** arranged the registration of companies involving figureheads implementing the registration (re-registration) of the companies.

While using material hardships of the figureheads, the **Individual A** proposed them a monetary reward for acting as a company founder and/or director without actual execution of related positional functions. The figureheads further had neither idea nor relation to operations of the shell companies.

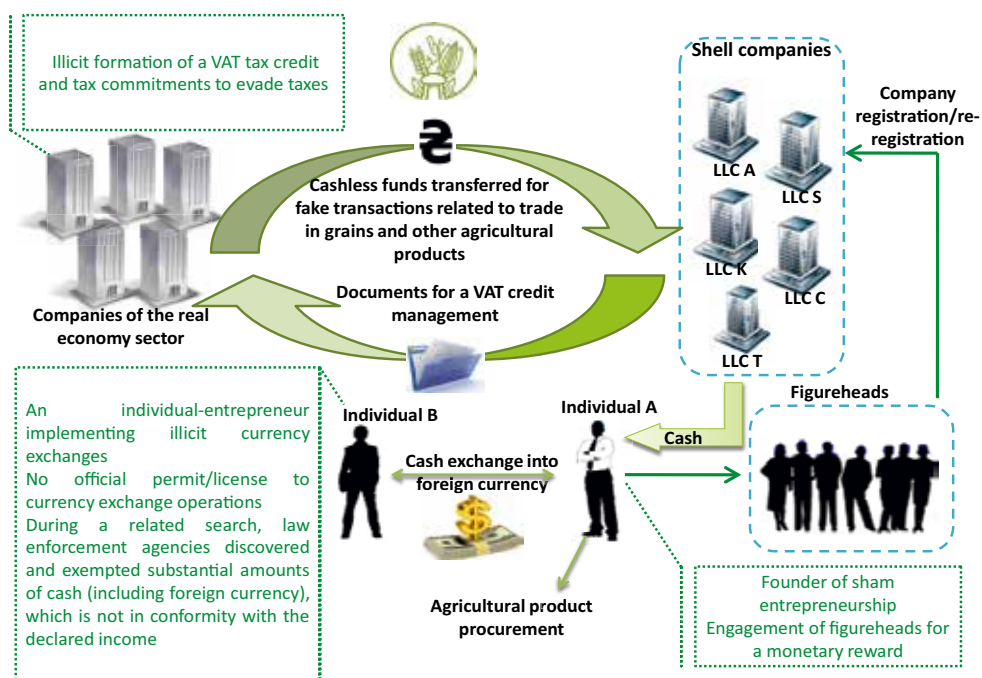
The **shell companies** implemented illicit formation of a VAT tax credit and tax commitments by companies of the real economy sector based on fake transactions related to trade in grains and other agricultural products.

In order to evade taxes, **companies of the real economy sector** transferred cashless funds to accounts of the companies controlled by the **Individual A**. The latter further converted them to cash, exchanged to foreign currency and partially used for procurement of agricultural products without any VAT payments.

During the related pre-trial investigation, a related law enforcement agency managed to establish that the **Individual A** implemented currency exchange while using services provided by the **Individual B** registered as a physical person-entrepreneur. At the same time, the **Individual B** has no official permit or license to trade in currencies.

During a related search at the **Individual B's**, law enforcement agencies discovered and exempted substantial amounts of cash (including foreign currency), which is not in conformity with the declared income.

A law enforcement agency is in the middle of a related investigation.



**Case 4.7. Cashless-to-cash asset conversions**

In accordance with an analysis implemented and information received from a law enforcement agency, SFMS has discovered a cashless-to-cash conversion scheme with the use of a group of legal entities and individuals.

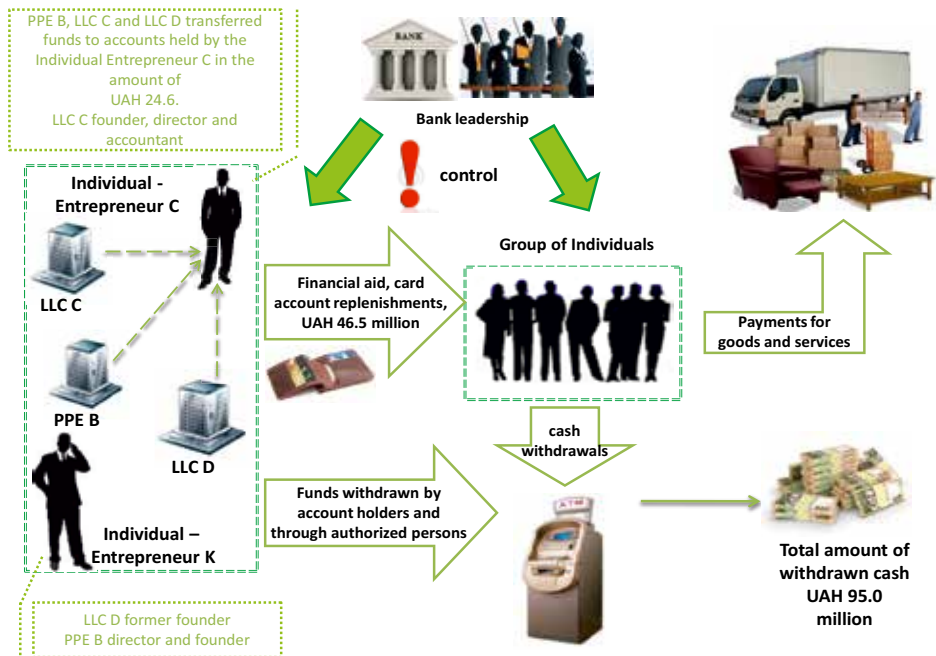
It has been established that funds from various legal entities were transferred to accounts of **3 legal entities** and **2 individuals-entrepreneurs** for various purposes, specifically, detailed as financial aid and payment for sunflower seeds, natural gas and services. The funds were later withdrawn in cash by account holders and authorized persons through an ATM network for procurement of agricultural products.

The scheme participants also transferred funds to card accounts of a group of individuals as financial aid and card account replenishments in the total amount of **UAH 46.5 million**. The funds were further withdrawn in cash or used as payments for goods and services. The total amount of funds converted to cash constitutes **UAH 95.0 million**.

According to the law enforcement agency, participation of a banking institution’s leadership member was established regarding control over activities of the illicit scheme participants.

The most of the above legal entities have sole founders and leadership. The companies were established with insubstantial authorized capital. Moreover, the **Individual-Entrepreneur C** has neither declared nor paid any taxes to the budget, similarly to the most of the companies involved in the scheme.

A law enforcement agency is in the middle of a related investigation.



#### **Case 4.8. Money laundering with the use of a banking institution**

---

During its surveillance activities, the National Bank established that a Bank had implemented a set of schemes related to cashless-to-cash conversions. The above transactions involved a number of legal entities, individuals-entrepreneurs and credit unions.

The scheme participants implemented a number of transactions aimed at multimillion transfers (more than UAH 200 million) to accounts held by the Bank clients (individuals) and further conversion of cashless proceeds to cash. According to financial status information available at the bank, the above clients were incapable of implementing such financial transactions.

Moreover, there were discovered a number of persons with their passports registered as lost, or when a passport's number and series were registered for another person.

According to the Bank documentation, the individuals involved in this scheme delegated their rights to personal account management to a sole client (physical person) with 500 additional payment cards issued by the Bank. According to law enforcement agencies, the passport of the above person was registered as stolen.

In 2016, the National Bank approved the withdrawal of a related banking license and liquidation of the above Bank for systematic violations in the AML/CFT field, specifically, in terms of risky operations in the field of financial monitoring.

A law enforcement agency is in the middle of a related investigation.





# **SECTION V**

## **USE OF PRESUMABLY SHELL COMPANIES IN MONEY LAUNDERING OR FINANCING OF TERRORISM**

---



**TERROROLOGICAL STUDIES 2017**



In many cases, operations implemented by conversion centres are used by presumably shell companies.

Withholding of information on beneficial ownership is the basis for the most of money laundering schemes and financing of terrorism. Proving beneficial ownership is one of the biggest challenges for financial institutions and competent bodies.

In its Guidance on Transparency and Beneficial Ownership 2014, FATF underlined specific mechanisms and sources for information on beneficial ownership of legal entities including company registries, financial (non-financial) institutions, a legal entity itself and other public administrations such as tax agencies or commissioned stock exchanges.

**The following indicators are specific for shell companies:**

- nominal owners and directors;
- insubstantial authorized capital;
- mass registration addresses;
- use of an email address only (often combined with nominal owners and directors);
- low personnel number (or only one person registered as an employee);
- tax defaults or available payables owed to employees.

**There are the following indicators that can be used to detect clients as such:**

**1. A client has no will to share personal information.**

**2. A client is reluctant to explain:**

- corporate history;
- information on the actual owner;
- origin of funds / authorized capital;
- specific ways to implement financial and economic operations;
- type of commercial relations with third parties (specifically those located at foreign jurisdictions).

**3. Individual or related persons:**

- insist on using an intermediary in all relations without a sound reason thereto;
- actively avoid personal communication without a sound reason thereto;
- are PEPs or having personal or business relations with a PEP;
- implement transactions involving younger or elderly persons;
- were previously convicted for criminal offences;
- it becomes known that they are defendants in a criminal investigation or having relations with criminals;
- implement operations incompatible with their client profiles.

#### 4. Legal entities:

- set simple banking relations through intermediaries;
- demonstrate sudden and unclear financial and economic operations after a lengthy period of stall after registration;
- registered under a name that doesn't point at its operations;
- registered under a name pointing at the fact that the company implements operations or services it does not provide;
- registered under a name which imitates the name of other companies, specifically, well-known corporations;
- registered at the address previously marked for numerous other companies or legal entities;
- have a great number of end beneficiaries and other controlling interests;
- registered / established at a jurisdiction considered risky in terms of money laundering or financing of terrorism;
- registered / established at a jurisdiction with low taxation rates;
- regularly transfer funds to jurisdictions with low taxation rates;
- implement a great number of financial transactions with a low number of recipients;
- keep close to zero balance at their accounts despite frequent incoming and outgoing transactions;
- use a great number of bank accounts;
- use bank accounts at various international jurisdictions without a sound reason thereto;
- require short-term or overly fast transactions, even if they bear unnecessary business risks;
- submit wrong documentation to a tax agency;
- submit wrong records or forged documents;
- have family members listed as end beneficial owners of the legal entities;
- employees of professional intermediary companies acting as nominal directors and shareholders.

#### The following financial transactions may prove their suspicious nature:

- deposits or withdrawals of substantial amounts in cash to (from) a bank account (s);
- transactions are implemented between two or more parties that are not visibly related by business or trade;
- transactions are implemented between family members of one or several parties without any legal basis for related business;
- transactions are implemented from an economic entity's account, but it appears that it is used for financing of personal purchases, including procurement of proceeds incompatible with a registered profile;
- transactions are implemented from an economic entity's account and contain a substantial amount of monetary proceeds as a deposit or financial aid, which is abnormal or incompatible with a company's profile;

- transactions are implemented in cycles (incoming and outgoing financial transactions are similar by their size, transferred and received by the same accounts, which signifies that incoming flows are returned with insignificant losses);
- transactions are implemented with the use of two legal entities with similar or equivalent directors, shareholders or beneficiaries;
- transactions consider a real estate transfer from an individual to a legal entity;
- transactions consider the use of several substantial money transfers to cover a loan or mortgage payments;
- transactions consider procurement of precious metals with cash;
- transactions consider a security transfer (to bearer) on an over-the-counter (OTC) market;
- loan or mortgage repaid early;
- loans are acquired from private third parties without any legal loan agreements, pawns or regular interest payments;
- an asset is procured with monetary funds and further used as a loan security for a brief period of time.

**Financial institutions and public administrations have access to simple tools facilitating identification of high-risk or suspicious clients. The above tools specifically include the following:**

- various registries including information on beneficial ownership;
- ownership and property rights registries;
- shareholder registry;
- commercial databases;
- declarations submitted by civil servants.

There are a number of new approaches to collection of data related to risk indicators to detect abnormal activities.

Since the most of financial transactions are implemented online, collection of information on IP addresses may contain useful data on a transaction customer and destination of a transaction. Moreover, analysis of IP addresses collected by a financial institution may define common characteristics and control relations when a single IP address is used for several clients and beneficial owners. Repeated IP addresses for several accounts may prove professional money laundering, and these accounts must be under enhanced monitoring.

While analyzing a location of an address provided by a client as well as external look of the address from outside (through web search engines like Google), an observer is often able to detect abnormalities demonstrating that a company is shell or an attempt to hide an actual client.

**The above abnormalities may include the following:**

- a location does not correspond to a client's financial profile;
- a location does not correspond to a company's business profile;

- a physical address does not correspond to a company's size and nature;
- an address is an email address.

The addresses proved to be abnormal require proper enhanced awareness measures and more attentive analysis of a related client.

Mass media are yet another tool to detect potential corruption, high-quality governmental contracts and high-quality corporate measures. Though mass media are not an indicator of a suspicious activity, they might be useful in identifying an abnormal or high-risk activity.





# **SECTION VI**

## **BUDGET FUND THEFT WITH FURTHER CONVERSION OF FUNDS TO CASH**

---



**TRIOLOGICAL STUDIES 2017**

Public administration remains a popular field for theft considering the amount of funds allocated to procurement of goods, labours and services to meet the needs of state-owned enterprises, facilities and organizations as well as companies with a state share.

Procurement of goods, services and labours from companies with a dubious or missing business record without any manufacturing capacity, warehousing premises or related personnel is quite popular. Such intermediaries cause overstated expenditures for procurement of goods, labours and services at the cost of state enterprises and companies with a state share.

Crimes within the budgetary sphere have become extremely relevant as of late. The above specifically relates to the defence industry since substantial budgetary allocations are referred to its financing.

There are the following most common ways of money theft and laundering at state enterprises:

- a state enterprise transfers funds for the benefit of companies (tender winners) related to the leadership of the above state enterprise. The above funds are later transferred to shell companies for further conversion to cash;
- a newly established economic entity without any employees or manufacturing capacity receives monetary proceeds from a state enterprise, and a part of those are later transferred for the benefit of intermediaries to meet terms and conditions of a related tender or to accounts held by public officials of the above state enterprise and related persons or companies;
- monetary proceeds received from a state enterprise for goods, labours or services are subsequently broken and dispersed between a high number of presumably shell companies. The above payments are usually detailed as financial aid, securities or debt transfer with further conversion to cash;
- a state enterprise transfers funds for the benefit of an economic entity without actual goods supply or service provision.

Cases with laundering money illicitly acquired from the state budget and state enterprises are provided below.

### Case 6.1. Budgetary funds theft and laundering through partial conversion to cash

---

In accordance with an analysis implemented, SFMS has discovered a state funds theft scheme with their further laundering.

During several years of procurement of food products for the needs of military servicemen, **state institutions** and **military bases** paid to presumably shell companies of dubious record.

Hence, the funds allocated to procurement of food products in the total amount of **UAH 49.8 million** were transferred to **LLC A**.

In accordance with an analysis implemented, further movement of the above funds has been established:

- **28%** of the total amount of acquired funds (UAH 14.0 million) was transferred for the benefit of various legal entities as a payment for canned products, other food products and similar product clusters;
- **72%** of the total amount of acquired funds (UAH 35.8 million) was transferred to other bank accounts, opened deposit accounts as well as for the benefit of a number of presumable shell economic entity as financial aid.

**UAH 2.6 million** of the total amount of funds used not for their intended purpose were withdrawn in cash and transferred to a physical person's account.

A law enforcement agency is in the middle of a related investigation.

### Case 6.2. State enterprise's funds embezzlement with the use of overstated prices and shell companies

---

Officials of a state enterprise in conspiracy with representatives of a resident commercial company took control over funds of the above state enterprise in the amount of **UAH 20.3 million** during the procurement of metal goods under preliminary overstated prices in 2015.

In order to launder the acquired money, the above officials entered into a criminal conspiracy with the persons in control over a number of shell companies and agreed to implement a set of economic transactions to procure drafting and adoption services for regulatory documentation, consulting, information, advertising, marketing, auditing and security services without any legal consequences or actual implementation of economic transactions. The procurement of the above services was not actually implemented but rather declared through a set of fake contracts and agreements. **5** resident companies involved in a controlled conversion centre providing illicit money laundering services as well as cashless-to-cash conversion services acted as counteragents of the above fictitious sale transactions.

**4** shell companies are registered at the same legal address. At the same time, the beneficiary of the above shell companies was promised a reward in the amount of 12% of the total value of fictitious relations for money laundering services and transfer to the accounts of the above companies.

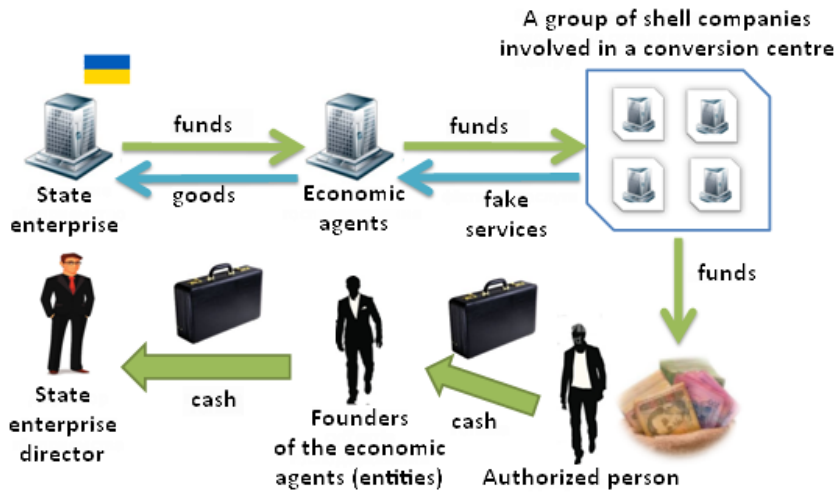
Moreover, in order to launder the above money, another controlled resident company was used apart from the 5 companies mentioned above. A consulting service contract was signed with that company.

As a result, the commercial company transferred from **UAH 125,000** to **UAH 2,000,000** to accounts of the shell companies to launder the above funds.

At the same time, the resident real economy company transferred a number of payments detailed as "consulting services" in the total amount of approximately **UAH 3.6 million** to the account of the controlled resident company.

A part of the above funds were withdrawn in cash by the resident company's officials. The related transactions were implemented with an interval of 1-3 days, and the amount of withdrawn cash per transaction was always the same – **UAH 299,300**.

Hence, the above activities allowed laundering money in the total amount of **UAH 20.3 million**. Real estate and personal property owned by the suspects in the amount of **UAH 7.5 million** were seized. A law enforcement agency has forwarded a related indictment to the court.





# **SECTION VII**

## **USE OF CASH BY PEP'S, RELATED PERSONS AND OTHER CIVIC SERVANTS**

---



**TRIOLOGICAL STUDIES 2017**

Activities of PEP's are based on wide powers and authorities allowing control over substantial financial flows within the state and taking part in money laundering schemes (budget fund embezzlement, bribery and so called "kickbacks") for further personal enrichment.

During financial investigations, a number of schemes were detected, but all of them had the same trait – cash, which complicates the process of discovering the origin of funds and allows integrating illicit gains into the real economy sector.

During this typological study, it was detected that the basic tools for money laundering involving a PEP and related persons were fake services, use of affiliated persons for pseudo-service provision, prepayments for goods and services to controlled persons with the following non-supply/non-provision and cashless-to-cash transfer of related funds or cash-to-cashless transfer when necessary.



### Case 7.1. Embezzlement of funds owned by financial institutions with the involvement of a legal entity controlled by a PEP and further conversion of the above funds to cash

In accordance with an analysis implemented, SFMS has detected a fund withdrawal scheme from banking institutions and a financial company for their further laundering.

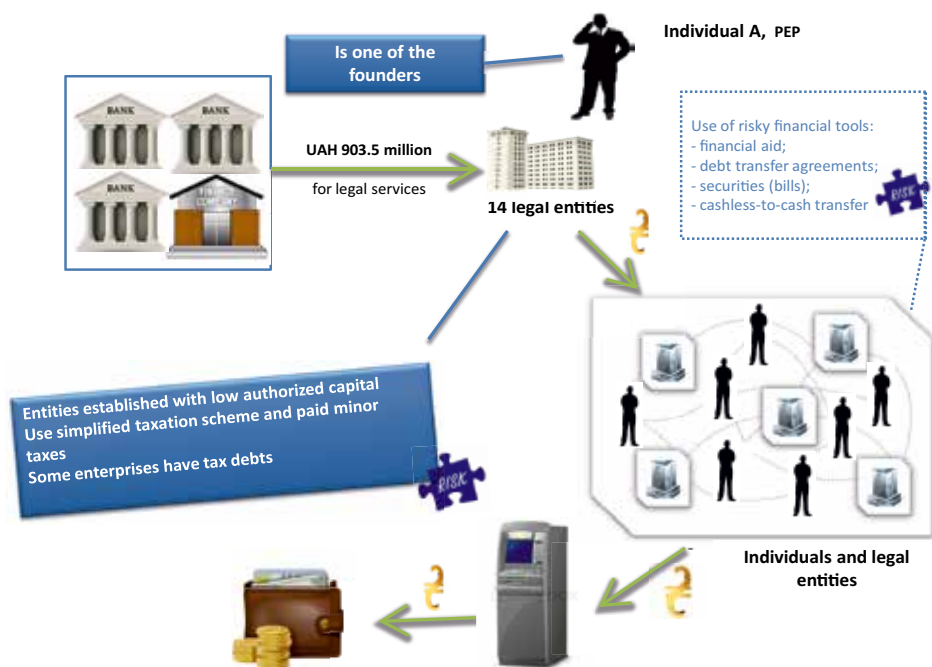
It has been established that **3** banking institutions and **1** financial company transferred funds in the total amount of **UAH 903.5 million** to accounts of **14 legal entities** with the same name and related by their founders and leadership as a payment for legal services, the value of which is difficult or impossible to define.

It is known that the above group of legal entities shares the following risks: the entities were established with a low amount of authorized capital, they were on a simplified taxation scheme and paid minor taxes, some enterprises had tax debts.

The peculiar fact is that one of the founders of the above entities is the **Individual A** who is PEP.

Further, the above **14 legal entities** referred the funds to other legal entities and individuals with the use of risky tools such as financial aid, debt transfer agreements, securities (bills) in order to arrange further conversion of funds into cash.

In order to avoid financial monitoring procedures, financial transactions aimed at cash retrieval were implemented in the amount that does not exceed the ceiling value for mandatory financial monitoring. A law enforcement agency is in the middle of a related investigation.



**Case 7.2. Money laundering by close relative of a PEP**

In accordance with an analysis implemented, SFMS has detected a money laundering scheme implemented by the **Citizen A** who is the wife of the **Citizen B**, a former top public official (the "A" civic service category).

It has been established that the **Citizen A** (seller) concluded a corporate rights trading agreement as of **23 March** regarding the **LLC D** with the **Citizen C** (buyer) for the amount of **UAH 54.0 million**.

It is known that the **LLC D** was registered on **10 March** (i. e., it had been active for as long as a month at the moment of the agreement signing) with the authorized capital in the amount of **UAH 54.0 million**. The company owns **2** premises and **2** land lots (estimated value of the above property constitutes UAH 6.5 million).

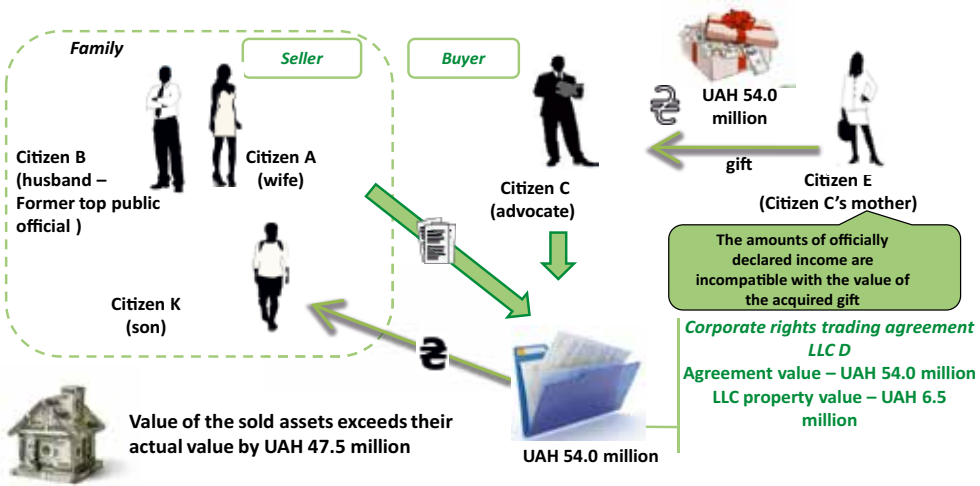
The **Citizen C** is the founder of 4 economic entities and operates in the field of advocating activities. The amount of declared income was **UAH 0.3 million** for 2003-2016. In order to fulfil the commitments taken under the above corporate rights trading agreement, he acquired a gift in the form of cash in the amount of **UAH 54.0 million** from his mother – the **Citizen E**.

The amounts of income officially declared by the **Citizen E** are incompatible with the presented gift value (in cash), which may demonstrate the use of concealed proceeds.

The value of sold **LLC D**'s proceeds exceeds their actual value by **UAH 47.5 million** or almost **7 times**.

The funds acquired from the sale of corporate rights were later acquired by the **Citizen A**'s son in cash on the day of the agreement's signing (**23 March**).

A law enforcement agency is in the middle of a related investigation.



### Case 7.3. Money laundering implemented by a person family-related to a judge with the use of a non-profit organization

In accordance with an analysis implemented, SFMS has detected a money laundering scheme implemented by an individual family-related to a judge.

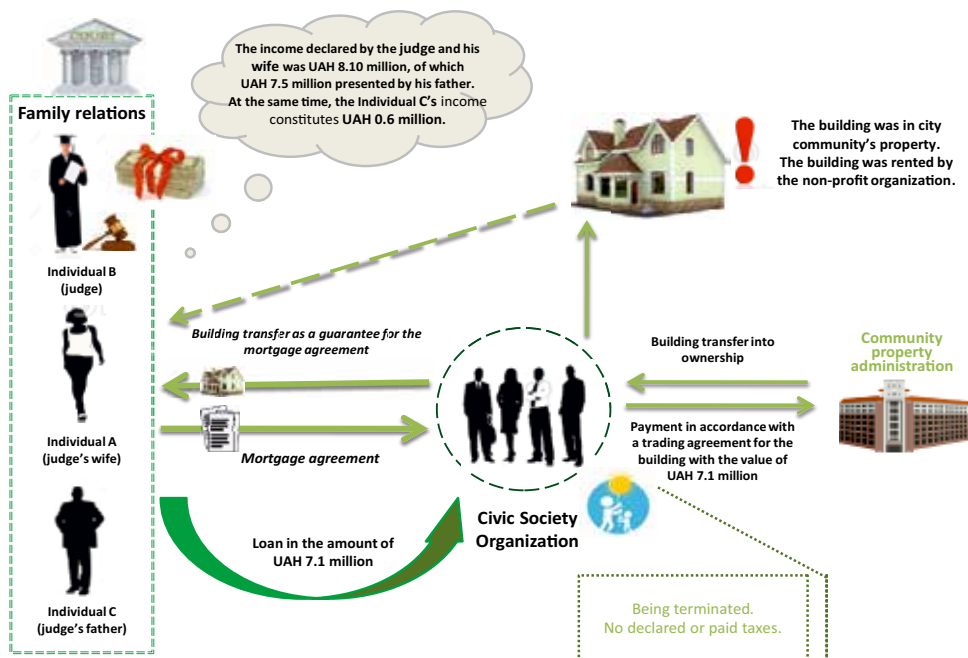
The **Individual A** deposited funds in cash to a personal account in the amount of **UAH 7.1 million** that were further transferred to a bank account of the **Non-Profit Organization M** and detailed as “loan provision”.

Information on the income officially earned by the **Individual A** is not available. At the same time, the husband of the above person, the **Individual B**, works as a judge and declared the fact of cash acquired as a gift from his father, the **Individual C**, in the amount of **UAH 7.5 million**.

The judge’s father declared his income in the amount of **UAH 0.6 million**, which is less than the amount of the gift by twelve times.

The **Non-Profit Organization M** entered a mortgage agreement with the **Individual A**. The item of the mortgage is a rented non-residential building with the total area of 467.9 m<sup>2</sup> owned by the city community. The above building was further procured by the **Non-Profit Organization M** from the community property administration under a trading agreement with the value of **UAH 7.1 million**. The above funds had been previously acquired from the **Individual A** and handed to the above person as a guarantee for the related loan agreement.

A law enforcement agency is in the middle of a related investigation.







# **SECTION VIII**

# **MONEY LAUNDERING THROUGH REAL ESTATE PROCUREMENTS**

---

TECHNOLOGICAL STUDIES 2017





Illicit gains can be invested into real estate as the most liquid environment and in order to form fixed capital.

As of today, the practice of registering ownership for real estate to offshore companies is used to conceal wealth. Hence, this phenomenon forms opportunities for further corruption spread and development as well as other offences.

Trading in real estate is closely related to the use of cash in Ukraine. However, transactions as such are supposed to be implemented in the cashless format as of now. At the same time, individuals have to replenish their accounts with cash before the procurement of real estate, and transactions of substantial value tend to have dubious origin.

There is also a scheme to procure real estate for cash under overstated prices, which is another way of money laundering.

Other overlapping processes with the above transactions may be using illicit cash for real estate building, construction and renovation to sell it afterwards.

### Case 8.1. Money laundering through the procurement of real estate

In accordance with an analysis implemented, SFMS has detected a money laundering scheme implemented by the **Citizen S** who is a PEP.

It has been established that the **Citizen S** entered a mortgage agreement to procure two apartments at an elite newly constructed residential building. The agreement value is as high as **USD 1.0 million**.

It is known that due to the mortgage, a notary set a ban to alienation of the above property. At the same time, the ban was lifted on the basis of a letter received from a banking institution due to payoff of the mortgage commitments in full and in the amount of **USD 1.0 million**.

The payment was implemented in five transfers from **USD 10,000** to **USD 500,000** deposited as cash through a bank cashier desk.

Before his public activities, the **Citizen S** was registered as an economic entity with official declared income in the amount of **UAH 1.0 million**. Moreover, the **Citizen S** earned income as wages in the amount of **UAH 1.75 million**.

The amounts of income officially declared by the **Citizen S** are not in conformity with the amounts of executed financial transactions.

The aforementioned scheme proves the **Citizen S** to have acquired concealed income with its further laundering through faking real estate procurement at the cost of credited funds.

A law enforcement agency is in the middle of a related investigation.





# **SECTION IX**

## **USE OF CASH IN THE SCHEMES RELATED TO TRADE IN NARCOTIC (PSYCHOTROPIC) SUBSTANCES, THEIR ANALOGUES AND PRECURSORS**

---

TRIPLOGICAL STUDIES 2017



Drug trafficking is illicit trade in banned narcotic substances, which is a multibillion criminal drug business at the same time.

Drug trafficking is most often related to other serious crimes such as human trafficking, organized sex work and travel paper forgery. This trade is most commonly used as a tool for financing of criminal and terrorist organizations due to its super profits and advantages acquired with relatively low time and capital burden.

In order to launder money, persons engaged in this criminal activity use a generic tool for this crime, which is the involvement of figureheads, including drug users. In order to evade official control procedures over financial transactions on behalf of the state, such criminals also use cryptocurrencies such as Bitcoin.



### Case 9.1. Laundering of proceeds from drug and psychotropic substance trafficking

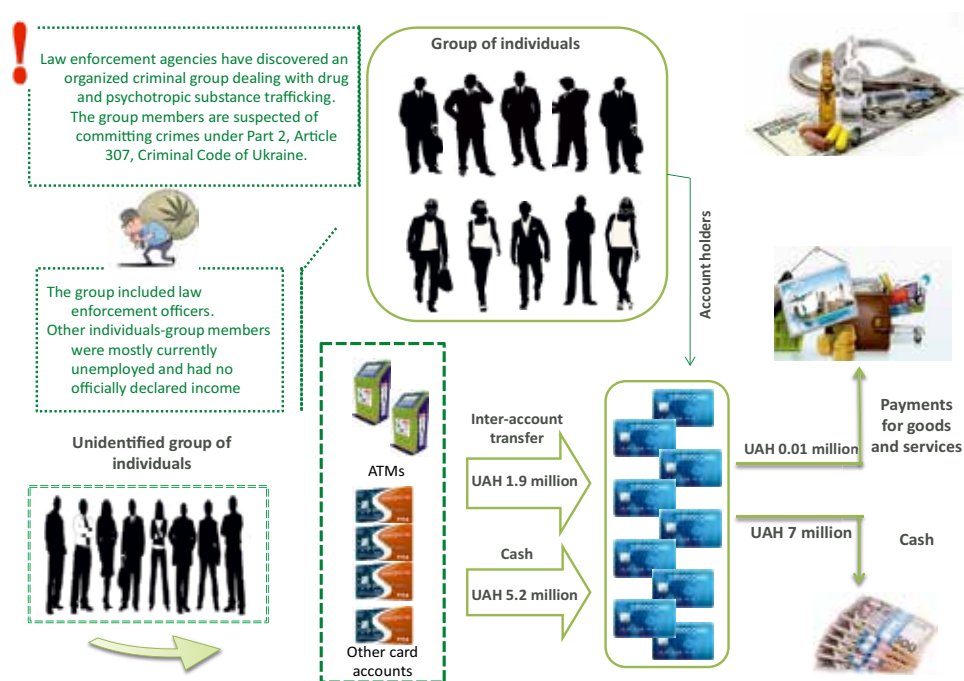
SFMS acquired information from a law enforcement agency on implication of a **group of individuals** in creation of an illicit drug and psychotropic substance trafficking scheme to acquire illicit gains in substantial amounts.

In accordance with an analysis of financial transactions implemented, SFMS has detected that funds in the amount of **UAH 1.9 million** had been transferred in the cashless format to card accounts held by **10 individuals** from card accounts of another group of individuals (inter-account transfers). Another **UAH 5.2 million** were transferred in cash through ATMs. The total amount of cashless/cash replenishments constituted **UAH 7.0 million**.

The above funds were further withdrawn in cash or used by account holders as payments for goods and services.

The **group of participants** of the above scheme included **individuals** who were employed by law enforcement agencies of Ukraine. Other **individuals-group members** were mostly currently unemployed and had no officially declared income.

A law enforcement agency is in the middle of a related investigation.



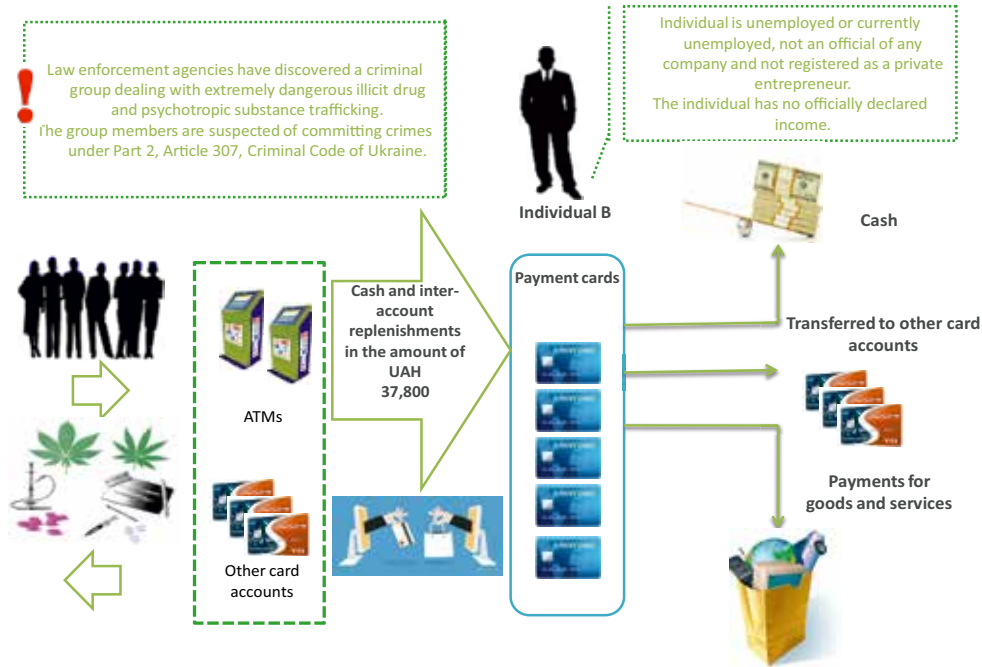
**Case 9.2. Laundering of proceeds earned through drug trafficking**

SFMS acquired information from a law enforcement agency on discovery of a criminal group dealing with extremely dangerous illicit drug and psychotropic substance trafficking to acquire and subsequently launder illicit proceeds.

In order to acquire the above funds, the group members used a payment card held by the **Individual B**.

In accordance with an analysis of the **Physical Person B's** implemented financial transactions, SFMS has detected that the above person holds several payment cards to receive cash deposited by various individuals through ATMs in the total amount of **UAH 37,800**. The funds were further withdrawn in cash and transferred to other card accounts or used by the **Individual B** to pay for goods and services. The **Individual B** is unemployed, and information on earned income is unavailable.

A law enforcement agency is in the middle of a related investigation.



### Case 9.3. Laundering of proceeds from precursor trafficking

The SFMS acquired information from a law enforcement agency on detection of a criminal group dealing with precursor trafficking and further money laundering.

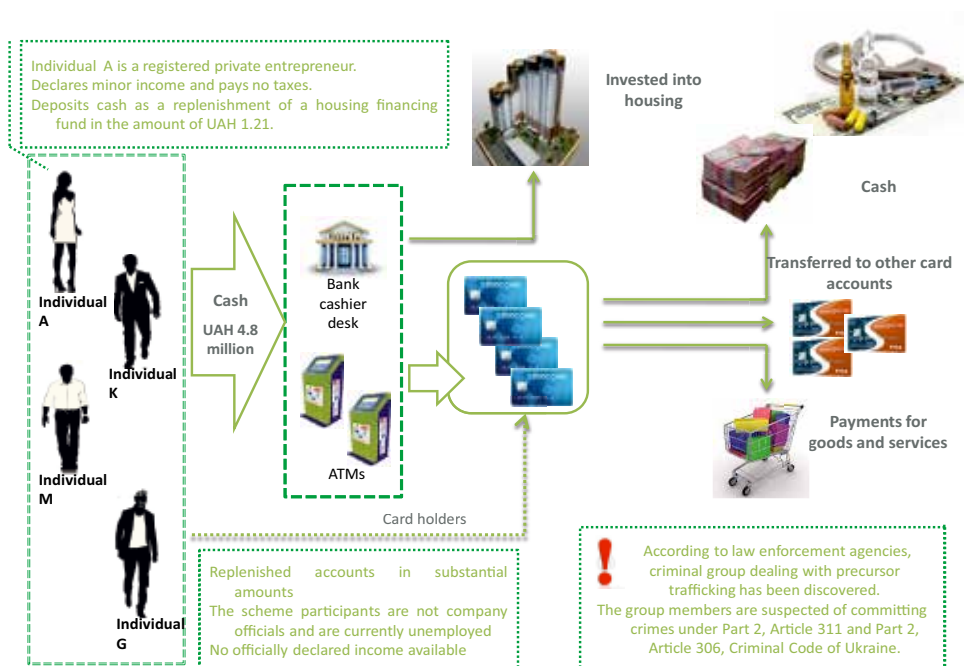
The organized group members used payment cards held by **4 individuals** to acquire their proceeds from illicit activities.

In accordance with an analysis of the **Individual A's**, **Individual K's**, **Individual M's** and **Individual G's** implemented financial transactions, the SFMS has established that the above persons deposited cash to their personal accounts and accounts of various economic entities through bank cashier desks in the total amount of **UAH 4.8 million**. The funds were further withdrawn in cash and transferred to other card accounts as well as used as payments for goods and services.

It has been established that the **Individual A** is a physical person-entrepreneur declaring minor income and paying no taxes. At the same time, the **Individual A** deposits cash as replenishments of a housing financing fund in the amount of **UAH 1.2 million**.

Other **individuals-members** of the criminal group are not company designated persons and are currently unemployed. No information on their official income is available.

A law enforcement agency is in the middle of a related investigation.



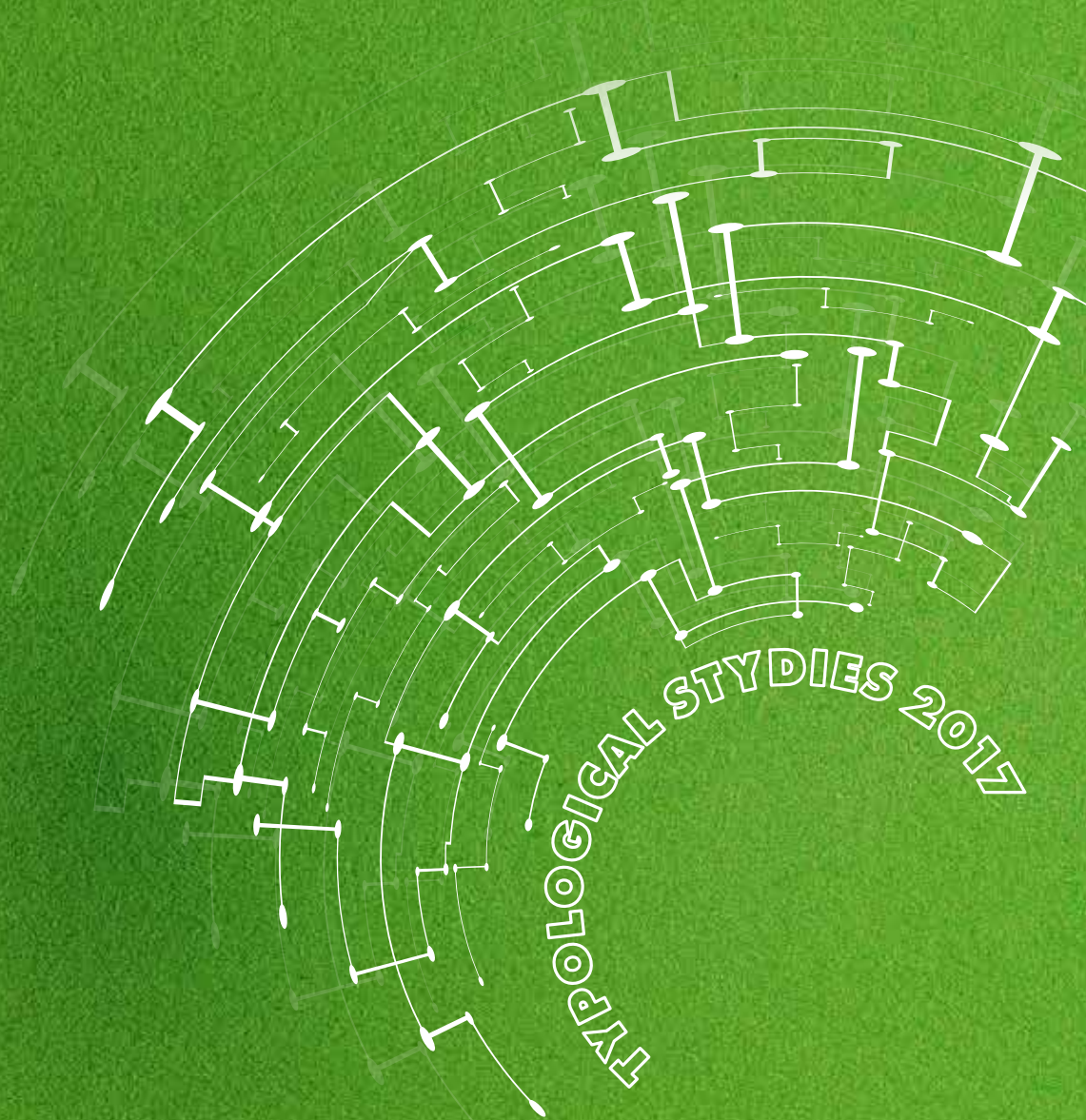




# SECTION X

## ILLICIT CASH MOVEMENT

---



TECHNOLOGICAL STUDIES 2017



As before, cash trafficking (smuggling) remains a very common tool. Despite the risks, this method is engaging due to full elimination of relations between funds and their origin in case of success.

Various stashes are used to move cash, including those created in luggage, vehicles as well as objects that can hold a substantial amount of cash without substantial changes in their original exterior.

Customs bodies registered **332** violations of customs rules by individuals moving across the state border of Ukraine since 2014 till 9 months of 2017.

Hence, when **entering** the territory of Ukraine, **175** persons violated customs rules. Specifically, this includes 25 persons in 2014, 89 persons in 2015 and 61 persons in 2016. **157** persons violated customs rules when **leaving** the territory of Ukraine. Specifically, this includes 17 persons in 2014, 97 persons in 2015 and 43 persons in 2016.

The biggest number of customs rules violations was detected during the state border crossings by individuals when entering Ukraine from the territory of the Russian Federation – 32 persons, Turkey – 30 persons, Israel – 13 persons and USA – 10 persons. When leaving Ukraine, the violations were detected for border crossings with the following countries: Poland – 42 persons, Russian Federation – 26 persons, Turkey – 14 persons and People’s Republic of China – 11 persons.

As a rule, perpetrators use an approach intrinsic for illicit movement of cash – figureheads or mules.

### Case 10.1. Money laundering with the use of a PEP outside Ukraine

In accordance with an analysis implemented, SFMS has detected a money laundering case outside Ukraine implemented by the **Individual S** who is a PEP.

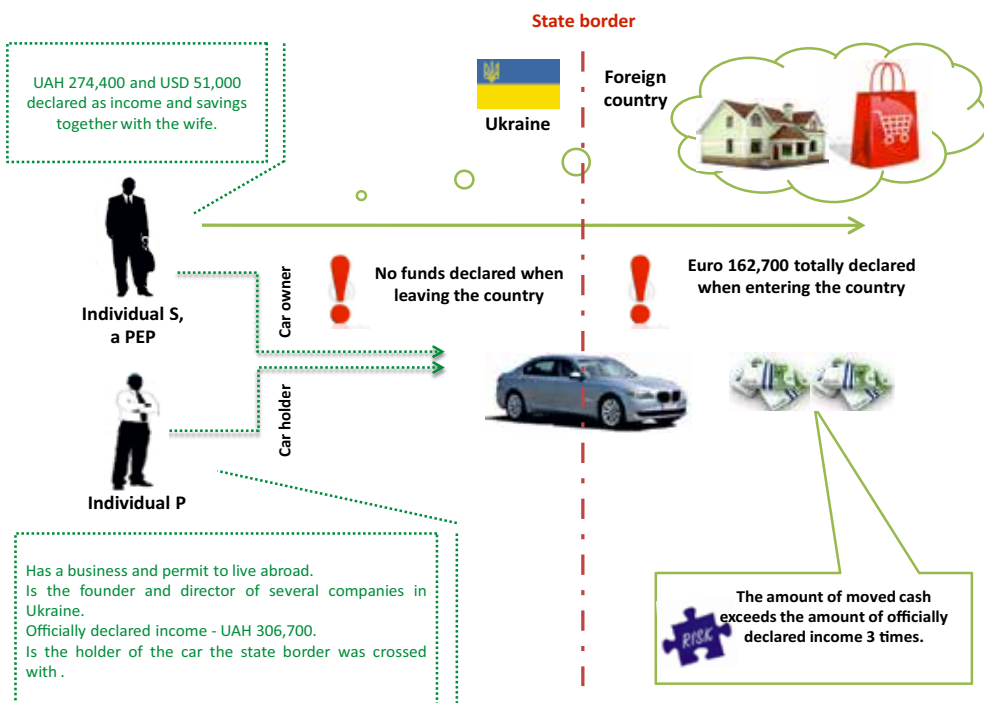
A financial intelligence unit of a foreign country notified SFMS of Ukraine of declaring cash in the total amount of **Euro 162,700** by the **Individual S** when entering the above country with a special note that the above funds were personal savings and would be used inside the above country for procurement of real estate and other purchases.

At the same time, according to the data from customs bodies of Ukraine, the **Individual S** had not declared any cash when leaving the territory of Ukraine.

The **Individual S** and his wife have their income and savings declared in the amount of **UAH 274,400** and **USD 51,000**. Therefore, the amount of moved cash exceeds the amount of income and savings officially declared by the **Individual S** by **three times**.

The car the state border was crossed with is owned by the **Individual S**, but this vehicle is not specified in a related declaration. The **Individual P** is registered as the holder of the above car, who is the founder and director of several companies in Ukraine with a permit to live abroad and the amount of officially declared income – **UAH 306,700**.

A law enforcement agency is in the middle of a related investigation.

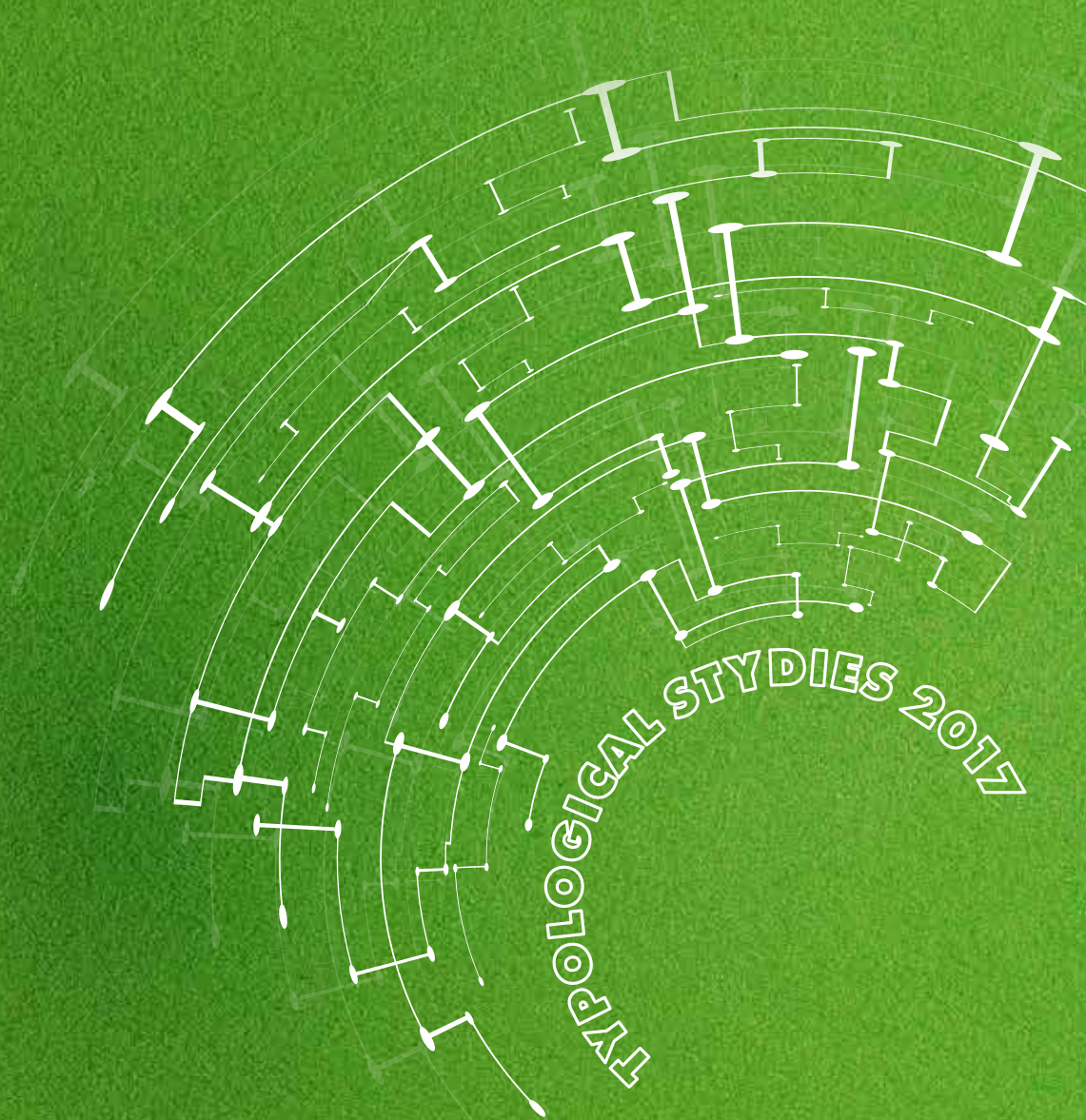




# SECTION XI

## CASH COMBINED WITH OTHER TOOLS

---



TRIOLOGICAL STUDIES 2017

With the aforementioned and studied schemes in mind, it is unequivocally possible to assert that criminals use cash as a tool to avoid leaving a financial track in all types of economic crimes when combined with other tools. The above renders identification of actual financial flow owners and controllers impossible.

**The following tools can be specified when combined with cash:**

- involvement of legal entities registered to men of straw;
- opening of a substantial number of accounts by the same legal entity or individual at different banking institutions;
- involvement of authorized persons from socially insecure population layers, persons with criminal record or those with lost IDs (men of straw
- in the implementation of financial transactions.

**Illicit proceeds can be integrated into a financial system as legal transactions as follows:**

- depositing cash to authorized capital of economic agents; depositing financial aid in cash by founders or officials to the accounts held by economic entities;
- depositing cash to deposit accounts of economic entities or individuals with further withdrawal thereof on the same or next day;
- depositing cash to deposit accounts of economic entities or individuals and further transfer of the right to withdrawal thereof under bank credit agreements;
- depositing cash to savings accounts of economic entities or individuals while issuing savings bearer certificates;
- depositing cash to accounts payable under bank credits (loans) for economic entities.

**During the typological study, it was also discovered that money laundering schemes involve combinations of cash use with other financial tools, specifically:**

- agreements on assignment of claims;
- use of men of straw for pseudo-service provision;
- fake securities (bills, shares or investment certificates);
- fake services, specifically, insurance proceeds under fictitious insured cases;
- financial and charitable aid;
- other types of loans.

The item of a financial transaction is an important element of cashless-to-cash operations, which can be different during both bank transfers between scheme participants and direct cashless-to-cash conversions, specifically:

- **for legal entities and individuals entrepreneurs:**
  - for procurement of goods, services and labours;
  - for economic and administrative needs;
  - entrepreneurial income;
  - procurement of securities from individuals;
  - loans/financial aid for employees.
- **for individuals:**
  - loans/financial aid;
  - replenishment of card accounts by third parties;
  - withdrawal of cash from card accounts with a dubious origin.



## CONCLUSION TO PART I

High cash flow is one of the risks for the “High financial system shadowization” threat defined during the NRA. Other important risk factors include inappropriate detection and elimination of shadowization factors, financial system offshoring, low public income level, low level of trust towards the financial system and capital flight from the country.

The scale of shadow economic relations in Ukraine remains close to critical. According to assessments implemented by the Ministry of Economic Development and Trade as well as those based on extrapolation, shadowization rates of the national economy are as high as 40% (UAH 740 billion in current prices or USD 31 billion as of the year 2015)<sup>7</sup>.

While summarizing the defined risk of “High cash flow”, it is worth mentioning that development of cashless payments results in decreased transaction demand for cash in Ukraine to be used for legal payments.

In order to minimize the above risk, it is necessary to take measures in order to ensure preventive actions for banks against risky (from the financial monitoring point of view) financial transactions.

In order to ensure efficient “High cash flow” risk management, there is a need in raising public financial literacy in the field of payment card use as well as improve convenience of utility payments, public service payments, tax payments and other regular payments with the use of payment cards. It is also necessary to raise the level of public trust towards the banking system of Ukraine and revise ceiling values for cash transactions.

In close cooperation with other stakeholders of the national anti-money laundering scene, the SFMS works to detect and eliminate current money laundering schemes.

With the above in mind as well as considering the fact that only a small part of cash remains in permanent circulation, basic attention is initially focused on detecting transactions related to deposits/withdrawals of cash that can be used to finance warfare in the East of Ukraine, cash transactions implemented by PEP’s and systematic cashless-to-cash transactions through bank cashier desks as well as elimination of “conversion centres”.

During several typological studies, it was detected that money laundering schemes with the use of cash tend to become more complicated and “up-to-date”. The above schemes involve electronic money and cryptocurrencies, and advanced technologies simplify cashless-to-cash transfers.

Each and every financial scheme with the use of cash equally combines other financial tools that may be different in their economic core. For instance, this relates to assignment of claims, insurance proceeds, purchase of securities, etc.

It is also worth mentioning that despite constantly upgraded and introduced legal restrictions on cash flows and improved control over financial system on behalf of public administrations, cash remains the “most favourite” asset for both legal entities and individuals.

<sup>7</sup> National Risk Assessment Progress Report published at the SFMS official website.

At the same time, the SFMS, law enforcement agencies and state regulators cooperate on the permanent basis to introduce new and upgrade current methods and approaches to detect money laundering cases with the use of cash.

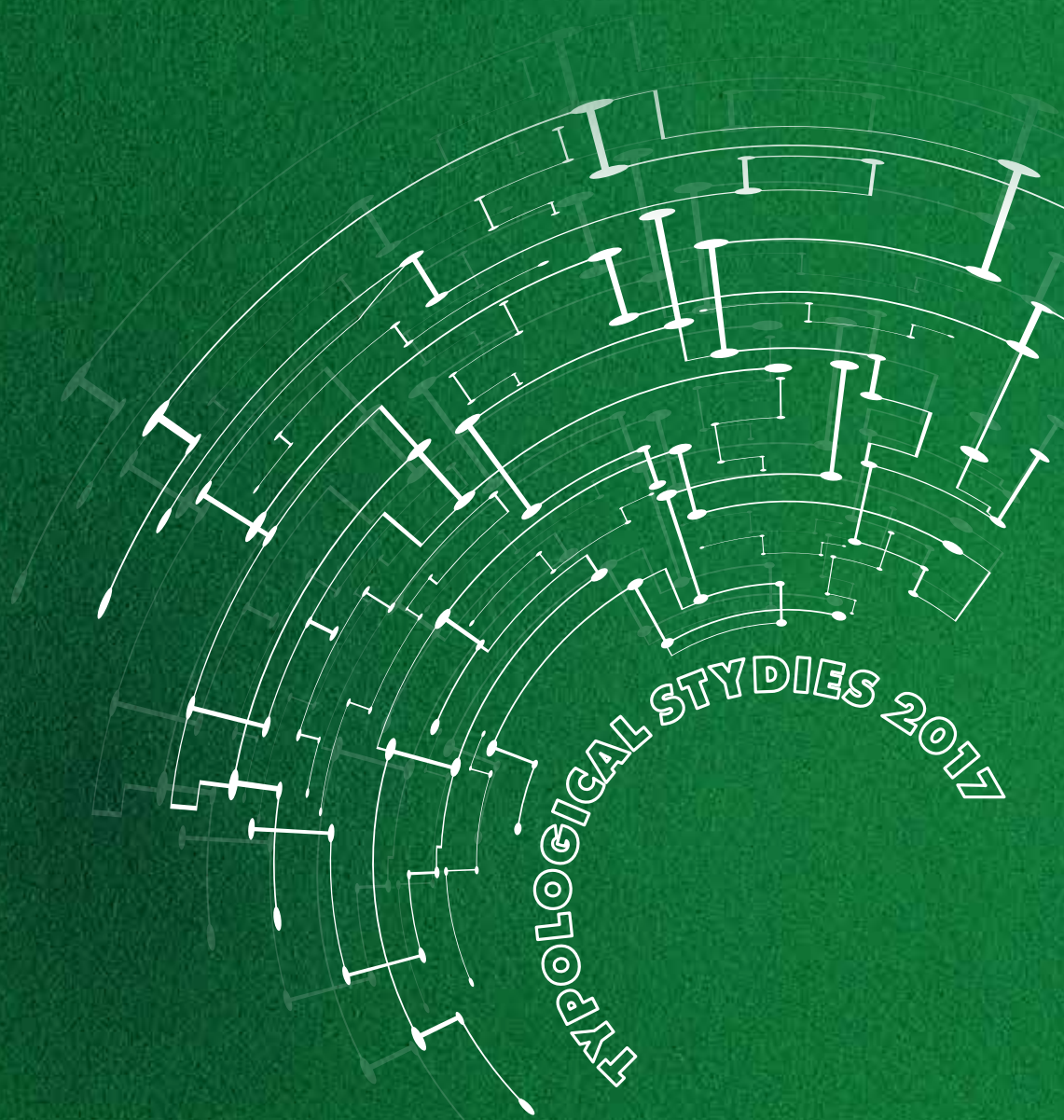
The use of the typological study when analyzing financial transactions will allow detecting illicit cash schemes in due time and prevent money laundering.

Hence, with the results of the National Risk Assessment as well as SFMS sectoral typological studies in mind, financial intermediaries are to minimize ML/FT risks.

# **PART II**

# **RISKS OF TERRORISM AND SEPARATISM**

---



## INTRODUCTION TO THE SECOND PART

By its nature, terrorism is the most socially dangerous and hard-to-predict phenomenon which has been widely spread all over the world in many of its forms recently.

Counterterrorism is defined as one of the priorities by UN and other international organizations. Terrorist organizations' activities pose a threat not only to national interests but the whole world safety. The basic requirements to counterterrorism (and financing thereof) are provided in the United Nations Security Council Resolution 1267 (1999) adopted on 15.10.1999. The above resolution is mandatory for all UN member states and aimed against the Taliban movement. Another Resolution 1373 (2001) adopted on 28.09.2001 is of universal nature and aimed against financing of terrorism in general comparing to the previous UNSC Resolution 1267 (1999).

Recent statistics proves the existence of approximately one thousand of groups and organizations using threats against population and seizure of power.

Today's terrorism is ever-changing by its purposes (it becomes multipurpose), forms and methods. It considers not only political impact but also elimination of national and religious fundamentals of a state and society, etc.

Separatism is yet another global issue both in Ukraine and all over the world. Separatism (Latin: *separates* – secession) is the will of communities, population groups or organizations to withdraw and detach as well as movement aimed at providing autonomous rights for a part of a country or full secession thereof to form a new state.

As of today, almost a half of the world's nations face actions that can be interpreted as separatism. The biggest number of the above cases occurs in Eurasia<sup>8</sup>.

The reasons for separatism occurrence may specifically include:

- external impact on behalf of interested foreign states;
- non-equal development of specific regions of a country;
- historical factors.

Current terrorism and separatism cannot be described as merely political phenomena. This notion mostly includes criminal terrorism and separatism. Such an activity is characterized not only by direct terrorist attacks but also financing of terrorist activities or separatism, procurement of weapons and ammunition, training and drilling for terrorists, arrangement of special terrorist cells, "lone wolf" recruitment, etc.

Terrorist succeed in adapting to fluent current conditions and finding new ways to meet their needs in financing, both legal and illegal. Legal financing sources may include funds acquired from charitable organizations or legal businesses as well as funds personally provided by terrorists themselves. Terrorists are also engaged in illicit activities of various types and scales – from petty

8 "International experience in fighting against separatism: Conclusions drawn for Ukraine", Analytical Report. [Electronic resource]. Access mode: [http://www.niss.gov.ua/content/articles/files/Separatism\\_druk-8a53a.pdf](http://www.niss.gov.ua/content/articles/files/Separatism_druk-8a53a.pdf)

crimes to organized fraud and drug trafficking. They may also acquire aid from states supporting terrorism; earn money in failed states and territories loyal to terrorist organizations, etc.

Terrorists and persons provoking terrorism have a huge amount of means at their disposal which allow moving monetary assets on both organizational and inter-organizational levels, involving cash couriers (mules), or using the financial sector. Charitable organizations and alternative systems for money transfers are also used to conceal (mask) funds purposed for financing of terrorism. Fitness and skills in finding alternative solutions intrinsic for terrorist organizations prove that any available money transfer may be used for illicit activities today.

The **general purpose** of this study is to analyze and generalize detected (standard and advanced) methods, ways, tools and schemes to finance terrorism and separatism. It also investigates into the risks, threats and vulnerabilities facilitating the financing of terrorism and separatism on the territory of Ukraine.

The typology uses experience earned by SFMS, national law enforcement authorities, public administrations, self-regulating organizations, international governmental and non-governmental organizations operating in the field of prevention of money laundering and terrorism financing.

It is the understanding of the process of management used in a terrorist organization or by persons provoking terrorism regarding their own assets which is an extremely important tool for efficient counteraction to financing of terrorist activity or separatism as well as elimination thereof.





# SECTION I

# RATIONALE

---



TRIOLOGICAL STUDIES 2017

Terrorism remains a significant threat, which is proved by recent terrorist attacks in many countries of the world. Counterterrorism is defined as one of the priority activities by UN. Special attention is focused on detection and efficient blockade of terrorism financing channels.

A similar to UN antiterrorism position was expressed by FATF under results of a plenary session held in June 2017 in Valencia (Spain, 21-23 June). The above position underlined the priority of fighting against terrorism financing.

The importance of counterterrorism activities was also emphasized by G20 leaders during their summit in July 2017. Their formal statement called for all countries of the world to eliminate all alternative sources of terrorism financing and cut the chains between organized crime and terrorist organizations.

The issue of separatism is one of the most complicated in the world since it is directly related to changes in current national borders and establishment of new states. As of today, there are no universal solutions thereto<sup>9</sup>.

Counteraction to proliferation of weapons of mass destruction is another relevant action for the world community.

The threat of proliferation of weapons of mass destruction is very serious and may result in complex consequences. The above activity may have many forms but in the end, it is brought down to transfer or export of technologies, software, services or knowledge that can be used in programs related to development of nuclear, chemical or biological weapons, including related delivery systems. This is what makes WMD proliferation a serious threat to the world's security.

Proliferation of WMD can be also controlled by terrorist organizations (groups) eager to use these weapons for terrorist attacks. There are assumptions that terrorist attempt to acquire chemical, radiology and nuclear weapons.

With the above in mind, proactive efforts to prevent financing of WMD proliferation should become an integral part of activities aimed at counteraction to terrorism and separatism. Special attention should be drawn to the ways financial aid is provided for terrorist organizations attempting to purchase and/or host WMD.

Updated methods for detection and prevention of financing of terrorism are of high relevance for Ukraine. The Antiterrorist Operation ongoing in ORDLO requires proactive events to fight against financing of terrorism and separatism.

Representatives of scientific society are actively involved in in-depth analysis of the situation in Ukraine within the risk context related to terrorism or separatism as well as search for relevant solutions.

<sup>9</sup> "International experience in fighting against separatism: Conclusions drawn for Ukraine", analytical report. [Electronic resource]. Access mode: [http://www.niss.gov.ua/content/articles/files/Separatism\\_druk-8a53a.pdf](http://www.niss.gov.ua/content/articles/files/Separatism_druk-8a53a.pdf)

Hence, the experts of the National Institute for Strategic Studies prepared 2 analytical works in 2016-2017 that were related to the issues at hand. Those are “Relevant issues of counterterrorist activities in the world and Ukraine” and “International experience in fighting against separatism: Conclusions drawn for Ukraine”.

The above studies specifically cover the following topics:

- relevant development trends of international terrorism;
- specific counterterrorist activities in the modern world;
- transformations of terrorist threats in Ukraine;
- international experience in the use of forced and peaceful methods to solve separatist-related conflicts;
- performance analysis of the use of specific methods and ways to counter terrorism;
- proposed solutions for the Donbas conflict considering techniques and methods that proved their efficiency in practice.

According to the NRA, SFMS has drafted a Report mainly focused on the definition (detection) of risks (threats) of financing of terrorism, their analysis and assessment. The Report is specifically focused on the following risks related to financing of terrorism and separatism:

- terrorism and separatism indicators;
- low-efficient activities implemented by competent bodies in the sphere of terrorism and separatism prevention;
- inefficient investigation of crimes related to money laundering, terrorism financing and proliferation of weapons of mass destruction;
- inefficient investigation of terrorism-related crimes;
- inadequate penalties for serious crimes related to money laundering, terrorism financing and proliferation of weapons of mass destruction;
- money laundering and terrorism financing through remote services;
- money laundering and terrorism financing through the gambling industry;
- use of non-profit organizations for money laundering, financing terrorism and proliferation of weapons of mass destruction.

SFMS and international organizations have implemented a number of typology studies related to counteraction to terrorism financing for the last several years.

In 2014, SFMS implemented a typology study titled “Relevant methods, ways and financial tools for terrorism financing and separatism”.

FATF implemented 5 international studies related to the above topics:

### 1. Terrorist Financing (February 2008)

The study was focused on the link between financial tools and antiterrorist activities. It was mentioned that performance of related efforts applied by public administrations to detect and investigate into terrorist activities could be significantly improved in case intelligence data could be used together with financial information. The study also highlighted traditional FT methods, ways and threats.

## 2. Risk of Terrorist Abuse in Non-Profit Organizations (June 2014)

The study explores the risk of using non-profit organizations for terrorism financing. It provides results of a case study dealing with the use of NPOs for illicit purposes, including FT.

## 3. Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL) (February 2015)

The study provides a brief overview of detected sources of income and types of financial activities implemented by ISIL. It also defines the basic sources of ISIL's proceeds and concurrent risks related to terrorism and terrorism financing.

## 4. Emerging Terrorist Financing Risks (October 2015)

The document explores new FT risks, methods and techniques emerging at the time of the study (2008). The work also assesses the relevance of traditional (as per the year of 2008) FT methods, techniques and threats.

## 5. Terrorist Financing in West and Central Africa (October 2016)

The study explores terrorism-related threats and vulnerabilities intrinsic for the Western and Central African regions. The work also delves into the use of monetary assets (including foreign currencies) in FT.

Despite constant changes in the quantitative and typological definition of terrorist groups as well as the threats they pose, the basic terrorists' needs in weapons, movement and use of funds remain.

However, changes in the sizes, contents and structures of terrorist organizations result in the changes of the ways they use to collect and manage financial resources (monetary assets) at once. Emerging challenges and threats require their constant investigation and analysis. Results of the above analysis are demonstrated as typology studies usually complementing the existing ones.

This typology study has used the results of the NRA in the field of prevention and counteraction to money laundering and terrorism financing finalized by SFMS in 2016 and involving all the participants of the national financial monitoring system: state regulators, law enforcement and intelligence authorities as well as self-regulating organizations and scientific experts. This practice is commonly accepted and used by numerous countries.

MONEYVAL 5<sup>th</sup> Round Evaluation Outcome was also used for the above purpose.



# **SECTION II**

## **TERRORIST-RELATED RISKS AND THREATS. GENERAL OVERVIEW**

---



**TRIOLOGICAL STUDIES 2017**

As mentioned above, FT counteraction remains a priority for international governmental and non-governmental organizations acting in the AML/CFT field.

According to several analytical studies, the following development trends of international terrorism may be defined<sup>10</sup>:

- permanent process of terrorism expansion worldwide, which resulted in a greater number of victims and growing feeling of insecurity and uncertainty among the population;
- significant financial losses and state resource reallocation;
- lowered activity of specific terrorist organizations;
- strengthened influence on political processes;
- use of advanced technologies in terrorist activities and their financing;
- impact of migration processes;
- increased global threat posed by ISIL and similar ultra-radical international terrorist organizations ("Al Qaeda", "Boko Haram", etc.).

The threats of terrorism and separatism are posed not only by large terrorist groups and organizations but also sourcing from local terrorist cells and "lone wolves" tending to commit terrorist attacks and tasks to significantly damage society. Due to the above, it is important to detect and eliminate financing networks of terrorist organizations of all types.

Risks of terrorism and separatism financing are based on a number of reasons, specifically:

- Ukrainian economy involves a wide range of cash use;
- weak control over the registration of legal entities and complexity of the verification algorithm for ultimate beneficial owners;
- great share of NPOs;
- currently set restrictions on verifications of legal entities;
- lack of control over specific parts of the state border.

Risks of terrorism and separatism financing are amplified due to the strategic and geographical location of Ukraine.

<sup>10</sup> "Relevant issues of counterterrorist activities in the world and Ukraine". Analytical report. [Electronic resource]. Access mode: [http://www.niss.gov.ua/content/articles/files/aktualniPitannya\\_press-1cl1ef.pdf](http://www.niss.gov.ua/content/articles/files/aktualniPitannya_press-1cl1ef.pdf)

## 2.1. Risks and threats related to terrorism and terrorism financing in Ukraine. Overview

The legal basis for counterterrorism and related financing consists of the Constitution of Ukraine, the Law of Ukraine "On fighting against terrorism" (№ 638-IV as of 20.03.2003), the Law of Ukraine "On prevention and counteraction to legalization (laundering) of the proceeds from crime, terrorism financing and proliferation of weapons of mass destruction" (№ 1702-VII as of 14.10.2014), Criminal Code of Ukraine (№ 2341-III as of 05.04.2001), International Convention for the Suppression of the Financing of Terrorism of 1999 (the Convention was ratified with the declaration of the Law of Ukraine № 149-IV as of 12.09.2002), Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the Convention was ratified with the declaration and warnings of the Law of Ukraine № 2698-VI as of 17.11.2010), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF recommendations of 2012 as well as other legal and regulatory acts adopted for the implementation of the Ukrainian legislation.

As of the last study of terrorism and its financing implemented by SFMS in 2014, its basic risk and threat trends haven't changed drastically.

Moreover, as of today, risks of terrorism and separatism expansion in Ukraine remain relevant considering a number of external and internal factors with negative impact on the national security. The external factors include increased activity of international terrorist organizations, formation of separatism-related ideas, organization and financing of activities aimed at violations of sovereignty and territorial integrity of the country. The internal ones are related to illicit flow of weapons and ammunition, radicalization of society, etc.

Under the counteraction to international terrorism, potential threats are caused by military warfare and terrorist activity in the Middle East, North Africa and Central Asia as well as proactive operations of terrorist organizations in EU member states.

Namely, as of today, Ukraine is considered a transit territory for transportation of militants to areas of armed conflicts, a safe haven for terrorist when hiding from law enforcement authorities of other countries, an area to engage and train their followers as well as to seek for financial and other material support to their illicit activities by the most of international terrorist and religious-extremist organizations (first of all, by ISIL).

The above results in attempts to expand the presence on the territory of Ukraine for persons who took part in military activities in squads commanded by international terrorist organizations as well as militias on the territory of other states as well as those on the international wanted list for committing crimes of terrorist nature. At the same time, current trends related to further illicit flight of the above persons to the European Union countries or participation in organization of general criminal groups in the territory of our country. The above inflicts substantial damage on the international image of Ukraine and contributes to destabilization of the national situation.

The specifics of terrorist activities in Ukraine initially involve incitement of separatist outbursts among the population in the east and south of Ukraine. The above activity involves a number of various methods:

- numerous threats (explosions, sabotage, etc. all over Ukraine);
- use of heavy weapon, including that against civilians;
- use of civilians as a "human shield" on the ORDLO territory (when fire is delivered from the territory of kindergartens, schools, residential premises, etc.);
- impeding the work of international organizations (UN, OSCE) on the ORDLO territory;
- use of various information sources, specifically, Internet, for propaganda, recruitment, financing, etc.

External sources are used to provoke separatist sentiments in Ukraine and its specific regions (first of all, in the east and south) through information campaigns and operations, provocations and incitement of related sentiments on sites, formation of negative image of the country among its population and discrediting amongst the international community.

Radicalization of social-political relations and huge amount of firearms in illicit circulation greatly increase terrorist threats. The cases of use or setting off explosive devices in Ukraine are not uncommon.

## 2.2. World trends to counter terrorism and terrorism financing

Analysis of antiterrorist activities of international and regional organizations as well as policies of several world countries allows specifying a number of relevant counterterrorism trends, including the following<sup>11</sup>:

- improved international interaction and information exchange between countries in terms of global fighting against terrorism;
- improved interagency interaction and information exchange between competent bodies in terms of fighting against terrorism on the national level;
- improved public awareness and preventive activities;
- use of advanced informational and technical tools;
- strengthened fight against terrorism financing;
- improved control over world's migration processes;
- improved legal framework taking current challenges and threats into account.

According to the "Terrorist Financing" FATF study, sizes and structures of terrorist organizations can be various: the biggest of those can have management boards similar to public administrations, while the smallest might not have any management units at all, which results in self-regulating activities.

The need in financing directly depends on the size of a terrorist organization and might significantly differ for many of them. Financing itself is required not only for specific terrorist attacks but also development of organizations, support to their current activities and formation of conditions for their further development.

At the same time, a significant share of the above financing usually consists of expenditures for current operations of a terrorist organization, recruitment of new members, planning and logistics.

In order to support operations of international terrorist networks and reach the goals set for them, there is a need in a well-developed infrastructure. In order to develop the above, promote terrorism-related ideology and finance legal activities to be used as a mask, there is a need in substantial funds.

<sup>11</sup> "Relevant issues of counterterrorist activities in the world and Ukraine". Analytical report. [Electronic resource]. Access mode: [http://www.niss.gov.ua/content/articles/files/aktualniPitannya\\_press-1cl ef. pdf](http://www.niss.gov.ua/content/articles/files/aktualniPitannya_press-1cl ef. pdf)



### 2.3. TF risks related to ISIL's activities

ISIL is a new form of a terrorist organization with financing thereof playing the key and central role in its operations.

ISIL's activities are different from the most of other terrorist organizations, especially in terms of financing for its operations, command and organizational structure. Hence, for instance, the biggest share of finances is coming from illicit activities on the occupied territories in Iraq and Syria and not donor and/or followers' donations.

ISIL is active on significant territories of Syria and Northern Iraq, which allows exploiting local population and financial resources through looting and theft. For this matter, ISIL uses various resources – from oil fields and banks to the use of engineering communications and taxation of local businesses. There are also evidence-based suspicions that ISIL trades in energy resources with the official Syrian government.

Another peculiarity (and the main difference at the same time) of ISIL is the fact that wealthy donors (followers) contribute only a tiny share of its financing.

According to international studies, there are established five major ISIL's financing sources:

1. illicit proceeds from criminal activities on the occupied territories: bank robberies, pillages, control over oil fields and oil refineries, looting of economic assets and illicit taxation of goods and cash in transit through the territory controlled by ISIL;
2. kidnapping for ransom;
3. donations, including those directly (or under the facilitation) from NPOs;
4. financial support, including that from foreign terrorist fighters, which involves collection of donations in their native countries for travelling to the territories controlled by ISIL, movement of cash by foreign terrorist fighters as well as money transferred by expatriates;
5. fundraising through current social media.

According to the US Government and FATF Report "Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)", at least 19,000 FTFs from more than 90 countries left their homelands and travelled for Syria and Iraq to join ISIL's ranks. Such a pool of foreign followers is a source of both physical and financial support for ISIL.

The above facts allow assuming there is a merit for ISIL when its followers establish recruitment centres all over the world.

## 2.4. Use of foreign militants in financing of terrorism

The issue related to FTFs is not new, but there are observed increased rates and scales of this phenomenon due to military activities in Syria and Iraq as well as the Antiterrorist Operation in Ukraine. The importance of efficient counteraction to the above threat is underlined by the UNSC Resolution 2178 (2014), which claims a serious concern on the establishment of international terrorist networks and elimination of threats posed by FTFs. The above is extremely relevant now since it considers the range of countries FTFs come from.

Despite the fact that today FTFs are not the key source of financing for international terrorist organizations (such as ISIL), they raise the terrorism threat level caused by the above groups. It is their activity considered one of the basic ways to provide both financial and HR support to terrorist groups by creating new threats related to terrorism financing. According to current assessments, self-financing and network financing aimed at recruitment and support are the most widely spread methods to raise funds for FTFs.

Self-financing of FTFs involves independent supply with financial and material resources. The funds raised this way can have both legal and illegal origin. The legal financing can include donations provided by relatives of terrorists (free-willing or unintentional), funds raised by intentionally established economic agents, sale of personal assets and credit resources. For instance, there are known cases when foreign combatants applied for petty loans to numerous financial institutions with no intent to repay them before travelling for an area of conflict.

There are also known cases when after having travelled for a conflict area, FTFs keep receiving their social aid transferred from their homelands. This deals either with the lack of awareness of related public administrations that a specific person is FTF or due to the lack of a legal basis to deprive such a person of the right to social aid due to his/her membership in a terrorist organization.

A typology study implemented by FATF provides an interesting source of terrorists' self-financing detected in Spain. Members of terrorist groups were used as figureheads in fraud schemes and VAT swindling in EU member states to acquire funds for covering their expenditures related to travel to an area of conflict. Proceeds from fraudulent activities as such are usually acquired in cash and further handed to terrorist-militants outside a related financial system.

Except for self-financing, numerous recruitment/support networks are also used for FTFs.

Recruitment networks and specific persons facilitate referrals of FTFs to conflict zones in order for them to join the ranks of terrorist formations. Relatives, friends or support groups also provide financial aid for FTFs after their departure for territories in war.

FTFs accomplices in their homelands are often related to their "colleagues" in the regions bordering with the areas of conflict. Moreover, there is also a strong link between FTFs support networks and criminal organizations.

Network support involves specific recruiters who often use social media for their work. People as such are often represented by members of extremist groups and their followers, or sometimes persons with a trivial relation to extremists. Apart from financial aid, recruitment/support networks also provide logistics support, including travelling and procurement of required means (including food products).

## 2.5. Counteraction to risks and threats related to terrorism and terrorism financing in Ukraine

During the period from 2014 till 6 months of 2017, law enforcement authorities referred 1,339 criminal proceedings regarding 2,369 physical persons<sup>12</sup> for commitment of crimes related to terrorist activities to the court, specifically those provided by Articles 258-258<sup>5</sup> Criminal Code of Ukraine:

- 58 criminal proceedings against 85 persons, 39 proceedings reviewed in court (3 judgements delivered, 3 persons convicted) in 2014;
- 425 criminal proceedings against 553 persons (including 19 persons as members of an organized group or criminal organization), 226 proceedings reviewed in court (69 judgements delivered, 52 persons convicted) in 2015;
- 464 criminal proceedings against 809 persons (including 66 persons as members of an organized group or criminal organization), 280 proceedings reviewed in court (135 judgements delivered, 103 persons convicted) in 2016;
- 392 criminal proceedings against 922 persons (including 61 persons as members of an organized group or criminal organization), 192 proceedings reviewed in court (65 judgements delivered, 55 persons convicted) in the first 6 months of 2017.

The Security Service of Ukraine, which is the major agency in the national system of counterterrorist activities, takes effective measures to counteract risks and threats posed by terrorism and separatism.

As a result of measures taken and investigative (search) activities implemented to prevent international terrorism in 2015-2017:

- 5 ISIL transnational logistics networks were shut down;
- an illicit scheme of providing combatants with passports of citizens of Ukraine to move abroad (including biometrical IDs) was detected;
- 23 transit points used as havens for combatants in various regions of Ukraine were eliminated;
- 86 ISIL and Al Qaeda members and followers were discovered, 17 of them were on the international wanted list;
- 9 ISIL members and followers brought to criminal justice in the field of terrorism and other related crimes (Articles 255, 258<sup>1</sup>, 258<sup>3</sup>, 263, 332 and 358 of the Criminal Code of Ukraine); indictments regarding 3 organizers of a transit channel for ISIL combatants referred to the court (Articles 258<sup>3</sup>, 258<sup>5</sup>, 263 and 358 of the Criminal Code of Ukraine);
- 53 ISIL members deported/forcibly returned from Ukraine;
- 1,355 ISIL followers are banned to enter Ukraine;
- an attempt of a car bomb attack (VBIED) in public place by ISIL followers prevented.

In order to counteract threats of the formation of terrorist and sabotage groups in the eastern and southern regions of the country with members selected from the local population and inspired by stakeholders residing in foreign countries in 2016, three subversion and reconnaissance groups related to illegal armed groups from ORDLO were detected and eliminated. 12 persons were

<sup>12</sup> Information provided in reports issued by the State Judicial Administration of Ukraine. According to the SIAU Order № 55 as of 05.06.2006 and Order № 153 as of 14.11.2012, courts only report once per half-year and annually. In case several crimes are committed, reporting is maintained in accordance with an article of the Criminal Code of Ukraine, which considers stricter sanctions.

detained; arms, ammunition and explosive devices planned for terrorist attacks in Odessa and Kherson Oblasts were seized.

In 2017, a deeply placed terrorist cell in preparations for a terrorist attack against one of the Members of Parliament of Ukraine was eliminated. When detaining the group members, explosive in the amount of approximately 1 kilogram (plastid), 5 electric detonators, Walther handgun with a silencer and approximately 100 ammos thereto, a combat quadcopter planned for a terrorist attack were seized.





# **SECTION III**

## **STANDARD METHODS, SCHEMES AND TOOLS FOR TERRORISM FINANCING**

---



**TRIOLOGICAL STUDIES 2017**

FT counteraction at both international and regional levels remains relevant.

As provided within the FATF typology, the financing needs of modern terrorist organizations need to be clarified in order to detect and get rid of the FT phenomenon as such.

Apart from funds required for committing actual terrorist attacks, there is a need in substantial amounts of money for development and current operations of a terrorist organization as well as its ideological impact. Substantial finances are also needed for propaganda of their views, rewards for combatants and their families, travel expenses, training of new members, bribes, document forgery as well as purchase of weapons and organization of terrorist attacks.

Terrorist organizations face a necessity to cover enormous expenses for masking their illicit activities as visually legal social or charitable operations.

The nature of financing of both terrorist attacks and assistance depends on the type of terrorist organizations that can be conveniently classified into 2 groups:

1. traditional organizations with a hierarchical structure similar to a state structure;
2. small-sized terrorist organizations without centralized management boards and operating autonomously.

The needs of terrorist organizations in financing are divided into 2 basic categories:

1. financing of specific terrorist operations (e. g., direct expenses for the implementation of specific operations);
2. financing of a more branched organizational activity aimed at development and maintenance of the current infrastructure to support and promote ideology of a terrorist organization.

While basing on results of studies related to the analysis of FT risks, there can be defined a certain pattern intrinsic for numerous terrorist organizations and the way they use raised funds.

Schematically, the elements of needs of terrorist organizations in financing can be demonstrated as follows:



Below goes a detailed description of financial need elements of terrorist organizations:

- equity fund financing: in case a terrorist group is a cell (component) of a bigger terrorist organization or has the same general purpose (common religious or ideological vision) with another terrorist unit (organization), it can approach that another organization for financial aid or provide it in return. For example, terrorist organizations raise funds this way to develop extremist websites;
- regular payments for current needs, accommodations and communications: terrorists need funds to cover their daily needs. A terrorist cell needs to be in touch with both its members and higher cells in a terrorist network. The lack of any other sources of income (hired labour or social aid) complicates their activities significantly;
- training, travels and logistics support of FTFs is yet another important part of activities for terrorist organizations for both ideological impact and development of practical skills. The funds allocated to financing of training and travels (including those spent on forged documents) are an important budget line for many terrorist organizations. The fact that even inexperienced terrorists acting as lone wolves and non-dependant on other organizations or higher command structures visited other countries for training or other drills directly before committing a terrorist attack is yet another indicator of importance to invest into training;
- direct expenses for terrorist attacks involve various resources required for committing a certain terrorist attack. For instance, this relates to self-made explosive substances, geographical maps, vehicles, tracking and observation devices, etc. Direct expenses for terrorist attacks are relatively low comparing to the damage they cause.

This study considers risks of terrorism and separatism financing in terms of traditional and advanced ways and methods.

Traditional ways (methods) to finance terrorism and separatism consist of legal sources (proceeds from a legal business or charitable organizations), use of illicitly gained funds (drug trafficking, ransoms, etc.), funds from the states encouraging terrorism as well as direct financing from terrorists.

The sources of financing mentioned above can be divided into two major types:

1. top-down (vertical) funding – substantial amounts of financial aid are provided on the centralized level: by states, companies, charitable organizations or credit and financing institutions supporting terrorism;
2. bottom-up financing – financing of terrorists' needs in a limited and dispersed way, for example, financing at the cost of terrorists themselves (their wages or social aid).

The use of legally sourced funds (charitable organizations or companies) as well as those directly invested by terrorists and their accomplices (wages, savings and social aid) resulted in a notion known as “delegalization”. The above means that legal means are used to recruit new staff or commit terrorist attacks.

### 3.1. Use of NPOs in terrorism financing

Depending on a country, NPOs may have various formats for legal entities. Such a claim is based on the types of activities and specifications of an organization which might pose a risk for their use in terrorism financing when combined with the factor that an organization operates on a non-commercial basis.

Such legal entities include formations or organizations that are primarily involved in collection and allocation of money to charitable tasks as well as religious, cultural, educational and social events.

NPOs play an important role in the world's economy, numerous national economies and social systems. Their efforts complement to activities of the public and private sectors.

Current international policy against financing of terrorism proves that terrorists (terrorist organizations) use the NPO sector for fund raising and transferring, logistics support, incentives for terrorists' recruitment or any other assistance for terrorist organizations and their activities.

Terrorists may also establish shell charitable facilities for fraud focused on fundraising.

Moreover, there are cases of engaging NPOs (including charitable organizations) in fundraising for terrorism financing. At the same time, such organizations can be used as both direct sources of income and masks for ML/FT activities.

#### **For reference**

*In accordance with the Law of Ukraine "On charity and charitable organizations" (hereinafter referred to as the "Law on Charity"), a charitable organization is a legal entity under private law with its statutory documents defining charitable activities in a single or several fields defined by the Law on Charity as the general purpose of its operations.*

*That means that a charitable organization by its nature is a non-governmental organization mainly focused on the implementation of charitable activities for the benefit of society or specific categories of citizens. The charitable activity itself can be characterized as volunteer disinterested activities of charitable organizations not aimed at earning proceeds from the above activities.*

*The Law on Charity defines the fundamentals of activities for charitable organizations that shall be specifically implemented in the format of:*

- *one-time financial, material and other assistance;*
- *systematic financial, material and other assistance;*
- *financing of specific target programs;*
- *assistance based on agreements (contracts) related to charitable activities;*
- *gifts or permits to use items of property free-of-charge (preferentially);*
- *permit to use a brand, emblem or other visualization symbols;*
- *taking responsibility for payments under free-of-charge, full or partial maintenance of charity items.*



Specifics of NPO activities make them attractive for terrorist organizations and vulnerable for criminal use for financing of terrorism and separatism. This deals with the fact that NPOs hold a high level of public trust and have access to financing sources which are difficult to control (e. g., charitable donations), and their operations often consider the use of a substantial amounts of cash.

NPOs are often used by terrorists for money transfers to finance terrorism. At the same time, the above operations can be mixed with legal financial flows, and their low volume cannot be claimed evidence of a decreased risk level.

Terrorist organizations consider NPO operations attractive since the latter have a wide range of influence all over the world.

Quite often, activities of such organizations are concentrated in the countries or territories that are directly close to regions of increased terrorist activities.

Another trait which makes NPOs attractive for terrorists is the status of non-financial institutions considering more lenient requirements to their operations comparing to crediting and financial facilities as well as economic agents. For example, those can be milder requirements to authorized, professional certification, verifications of bio data of employees and chair members during the registration, continuous document management, etc.

The specifics of NPO activities results in the occurrence of numerous risks that can be detected and used for terrorists financing.

There can be defined three major specifications of illicit NPO use:

- change in the purpose of NPO donations (including those for a charitable organization);
- use of a shell entity pretending to be legal to mask its activities and in fact used by a terrorist group;
- so-called "large-scale use", for instance, when an NPO is actually used for purchase of food products for orphans, but it does that through a special terrorist organization.

Change in the purpose of NPO donations is nothing else but illicit flight of funds collected through donations. The latter are initially collected for legal goals but then used for financing of illicit operations, specifically, terrorism financing. Such fraud can be practiced together with actual charity, and all other types of a charitable organization's activities can remain legal.

Shell NPOs working as legal organizations are often used for terrorism and separatism financing.



**Case Study 3.1.1. Use of shell civic society organizations for terrorism and separatism financing**

SFMS has detected a financing scheme of the Ukrainian **NGO B** implemented by foreign organizations to host information events in Ukraine for information propaganda.

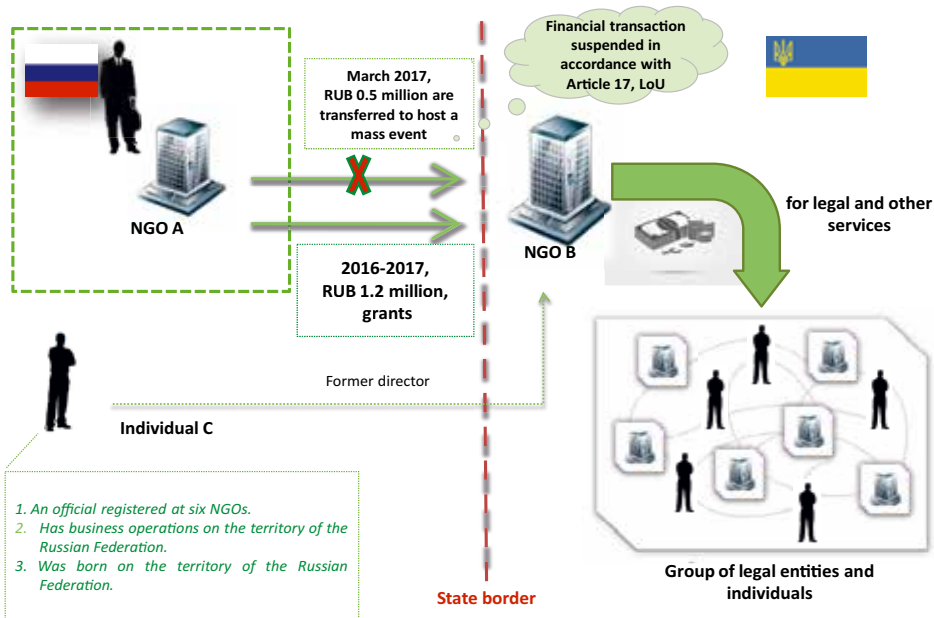
In March 2017, there was an attempt to transfer money in the non-return grant format in the amount of **RUB 0.5 million** for the benefit of the Ukrainian **NGO B** from the foreign **NGO A** to implement a non-sanctioned mass event on the territory of Ukraine.

In terms of the above financial transaction, a decision was made to suspend it.

During the related investigation, it was established that the **NGO B** received regular money transfers from foreign charitable funds and civic society organizations in 2016-2017 as grants in the total amount of **RUB 1.2 million**. The funds were further converted to UAH and transferred to individuals and legal entities for provided legal and other services.

The **Individual C** earned income from a political party subordinated to political elites of a foreign country. Hence, the money provided by the foreign **NGO A** for the implementation of mass events can be as well purposed for waging a hybrid war against Ukraine through informational propaganda.

Law enforcement authorities are in the middle of a related criminal proceeding.



*Below goes a list of other scenarios of illicit use of charitable organizations.*

### **Case Study 3.1.2. Use of a charitable organization for terrorism financing**

---

A **Country B's** FIU received a message on suspicious operations regarding the **Individual A** to donate a substantial amount of money to the account of a charitable organization. The **Individual A** had a related Power of Attorney to enjoy the right to manage the above funds and further transfer them to a notary as an advance payment for real estate purchase.

According to a related investigation, the following was discovered.

The funds available at the above NPO's account were accumulated from numerous cash deposits (possibly charitable deposits and donations) and direct transfers from the **Individual A's account**. Next, verification of the **Individual A's** account demonstrated that the funds deposited to his account were accumulated from deposits from private persons submitted as donations.

Transfers from the **Individual A's** account were implemented for the benefit of the above NPO, and international transfers – for the benefit of the **Individual C**. Police has established that the **Individual A** had contacts with persons related to a terrorist organization with the **Individual C** in its ranks.

Law enforcement authorities have established that the charitable organization actually collected money for charity, but it was used as a cover to accumulate funds for terrorism financing and next – to transfer a part of the above funds to terrorists, the **Individual A's** accomplices.

Law enforcement authorities are in the middle of a related investigation.

### **Case Study 3.1.3. Use of a charitable organization related to terrorists for fraud**

---

The **NGO X** has managed to collect substantial funds for the last two years while receiving financial aid from one of the governmental institutions.

Intelligence agencies have detected that the leadership of the **NGO X** were connected to extremist groups from a foreign country.

Moreover, there were other indicators of fraud activities: excessively high number of students in this organization (respectively, higher rates of funds requested from a governmental institution).

Law enforcement authorities are in the middle of a related investigation.

### **Case Study 3.1.4 Use of a charitable organization for recruitment of terrorists**

---

After comparison of the client database with the lists of persons related to terrorism, employees of one of the banks from the European **Country B** detected an NPO from the European **Country C** that had an account at their bank and was in the above lists. Basing on the discovered information, the bank employees submitted a related message to a **Country B's** FIU.

The account of the above organization was opened a couple of years ago, and most of time, it remained low-active. Subsequently, the number of transactions increased dramatically. The transactions were made in the format of cash deposits (with a rather substantial total amount) made by different individuals. The funds were later withdrawn from the account in cash.

As a result of the investigation implemented by the FIU of the **Country B**, the following was detected:

- after analysis of the information provided by security services of the **Country C**, the FIU employees of the **Country B** concluded that the above NPO was one of the contact points in the **Country C** that was recruiting and sending FTFs to war zones in the Middle East;
- it was also established that several individuals persons with the right to authorize transactions of the organization's were connected to a terrorist group.

Law enforcement authorities are in the middle of a related investigation.

### Case Study 3.1.5. Use of a recruitment/support network

---

In May 2015, law enforcement authorities detained the **Citizen E** from the Republic of Azerbaijan, who was an active ISIL follower, in the city of Kharkiv.

While in Kharkiv and Kharkiv Oblast, the **Citizen E** established and ensured constant operations of a transit channel for ISIL members from Caucasian countries and Central Asia through the territory of Ukraine and Turkey to the Syrian-Iraqi zone from October 2013 to May 2015 for their further participation in military activities in the ranks of the above terrorist organization as well as a return route for them.

The aforementioned **Citizen E** also provided foreign terrorist-militants with material and financial resources (monetary assets), places of temporary stay, IDs and travel documents to leave Ukraine as well as coordinated border crossing by the above persons to Ukraine.

When detained, the **Citizen E** possessed **USD 30,000** which were planned for further illicit use.

It was also established that the organizers of the above network financed the transborder transfer of a militant who took part in terrorist activities in Syria and passed full course of sabotage and mining-explosive training in terrorist groups related to ISIL to one of the Central Asian countries. The above combatant was detained in the territory of the above country during the implementation of a terrorist attack.

UNSC was sent requests on inclusion of two suspects under the above proceeding to a related sanction list.

A related indictment under this proceeding has been referred to court. A related court hearing is underway.

### Case Study 3.1.6. ISIL-related case

---

Approximately in the middle of 2014, the **Citizen S** facilitated to convert the **Citizen K** to Islam for her further engagement into ISIL's extremist activities.

In May 2015, the **Citizen K** and her common law husband (a Jordanian national and a Muslim by faith), the **Citizen D**, joined ISIL ranks to commit a terrorist attack.

In June 2015, when following given instructions and guidelines of ISIL members, the above persons reached the Syrian-Iraqi warfare conflict zone controlled by ISIL FTFs and followers.

In September 2015, under further influence of the leadership of the terrorist organization, the **Citizen D** in conspiracy with other persons committed a terrorist attack in Bagdad (the Republic of Iraq) suburbs, which resulted in deaths of at least 20 persons and wounding at least 60 citizens of the Republic of Iraq.

The related investigations are underway.

## 3.2. Indirect terrorism financing

Measures taken by public administrations of Ukraine make some terrorist organizations to transfer to the so called “indirect” terrorism financing when a person or a group of persons financing terrorism engage other or manage other persons to collect funds and/or other assets.

At times, indirect terrorism financing considers direct material support to terrorists, meaning supplies of the necessary equipment (including that for military purposes), ammunition, food products, weapons, etc.

Below goes a list of other case studies of indirect FT.

### Case Study 3.2.1. Indirect FT

During a pre-trial investigation in a criminal proceeding, it was established that the **Citizen D** sent a cargo for the total amount of UAH 11,000 (approximately USD 450) in October 2014-January 2015 via the Delivery Service A for financial and material support to specific terrorists of one of the terrorist organizations in ORDLO.

A judicial body convicted the **Citizen D** to imprisonment for terrorism financing.

### Case Study 3.2.2. Indirect FT

A pre-trial investigation is underway under a criminal proceeding in accordance with Part 3 Article 258<sup>5</sup> of the Criminal Code of Ukraine (financing of terrorism) regarding a number of charitable organizations from Ukraine implementing financial and material support to a number of terrorist organizations in ORDLO through the transfer of goods and funds masked as aid for victims of aggression on the territories temporarily not controlled by the Government of Ukraine in Donetsk and Lugansk Oblasts.

### Case Study 3.2.3. Indirect FT

In accordance with the available information, the **Citizen of Ukraine K** residing in the city of Donetsk arranged the trade in medicines in ORDLO previously procured in Ukraine in order to finance terrorist groups on the temporarily occupied territory of Donetsk Oblast. The income earned from the sales was allocated to financing of the above terrorist groups.

The **Citizen K** is suspected of committing a crime under Part 2 Article 258<sup>5</sup> of the Criminal Code of Ukraine.

The law enforcement authorities are in the middle of a related investigation.

### Case Study 3.2.4. Indirect FT

It has been established that the **Individual-Entrepreneur M** paid the so called “monthly taxes” to terrorist organizations on the temporarily occupied territory of Donetsk Oblast when implementing passenger traffic between Ukraine and ORDLO.

A related investigation is underway.

### Case Study 3.2.5. Indirect FT

---

Illicit operations of officials from the **LLC Z** procuring food products in the **Country R** without related customs documentation have been stopped.

The food products were later transported to support illicit operations of illegal armed groups on the temporary occupied territory of Donetsk Oblast.

A related investigation is underway.

### Case Study 3.2.6. Indirect FT

---

A pre-trial investigation is underway in a criminal proceeding related to a fact of criminal violations committed by a number of legal entities in accordance with Part 1 Article 258<sup>5</sup> of the Criminal Code of Ukraine.

During the investigation, it was established that officials of the **PJSC L** implement activities to introduce a strategy on retrieving the negative VAT value as a substantial amount for an owner of the **PJSC T** in the **Country R** (under special economic sanctions for 1 year in accordance with the decision made by the National Security and Defence Council of Ukraine).

The acquired funds were further used to support illegal armed groups as well as coverage of so called "taxes" on the temporary occupied territories of Lugansk Oblast.

Moreover, representatives of the above company established a so called "mirror company", the **PJSC L-L** at the basic of the integrate property of the PJSC L. The above mirror company paid the so called "taxes" and provided premises for renovations (maintenance) of military machinery owned by illegal armed groups, thus supporting and financing terrorist organizations on the temporary occupied territories in Lugansk Oblast.

The law enforcement authorities are in the middle of a related investigation.



### 3.3. FT sources

In specific cases, terrorist groups provide financing from their own sources, which includes costs provided by terrorists' families and other legal tools. Funds required for small-scale terrorist attacks can be raised by sole terrorists and terrorist networks supporting them while using shadow financial flows, illicit fund transfer channels, savings, credit resources and income of controlled companies.

The basic sources of shadow financial flows to support terrorists in Ukraine can include the following:

- activities of sole groups to support illegal armed groups in ORDLO with necessary resources (including funds);
- funds acquired from corruption activities, looting and embezzlement of state funds and property;
- funds acquired from financial and industrial groups;
- funds acquired from trade in contraband and/or counterfeit products;
- funds acquired as a result of destruction of industrial objects in ORDLO (destruction of industrial objects to earn proceeds through the trade in ferrous and non-ferrous metals);
- extortions implemented by terrorists at control points to ORDLO and checkpoints in ORDLO;
- provision of new specific illicit services, specifically, aid in registering the status of an internally moved person in order to acquire social payments as per the valid legislation of Ukraine.

The implemented NRA in the field of prevention and counteraction to money laundering and terrorism financing allowed detecting the following illicit channels for movement of funds:

- money transfers to card accounts held by terrorists (separatists);
- extortion of financial aid from economic agents for the needs of the so called "ORDLO officials";
- conversion centres;
- fundraising in social networks masked as social aid;
- money transfers through the use of payment systems.

#### Case Study 3.3.1. Terrorist organization's self-financing

In order to commit a successful terrorist attack at a transport infrastructure object of a European capital, a small-sized terrorist cell was able to raise the required amount in case while the bigger part of the cell was out of focus and not related to any terrorist and other illicit activities.

The **Citizen A**, who provided the biggest share of raised funds, had a crystal clear reputation and was not suspected of any illicit activities. He also had an ideal credit ranking with several deposits of small amounts in banking institutions. The preparation for the terrorist attack was implemented in two phases: during a month approximately in 10 months before the date of the attack and starting in 4 months before the attack till the attack itself.

The **Citizen B** made several purchases in several months before the terrorist attack. He used cheques as payments later returned by the bank due to insufficient funds on his account. The **Citizen B's** activities provoked a suspicion, which resulted in the bank representatives visiting the **Citizen B's** residence next day after the terrorist attack.

The total amount of raised funds constituted approximately **EUR 11,000**.

The law enforcement authorities are in the middle of a related investigation.

### Case Study 3.3.2. Terrorist organization's self-financing

---

There was established the identity of the **Citizen** of the French Republic who was not sharing the liberal migration policy of the European Union member-states and was a radical person.

In order to bring attention of the EU population to the migration crisis issue, the above **Citizen**, together with other persons, decided to commit arsons and explosions at specific infrastructure objects and other location on the territory of the French Republic. For that reason, he procured various pieces of firearms, ammunition and explosives on the territory of Ukraine (without a proper legal permission). In order to commit terrorist attacks, he selected approximately 15 potential objects – vehicles, a tax police administrative building, mosques, cities, payment systems and video surveillance systems on international roadways.

In order to purchase the above weapons, ammunition and explosives in April 2016, the above **Citizen** of the French Republic arrived at Ukraine and procured those illicitly at the cost of his personal funds. The person was detained when trying to move those out of Ukraine.

The above **Citizen** of the French Republic was laid with a related charge, and his case is being reviewed at the court.

### 3.4. Illicit funds in terrorism financing

Some terrorist groups acquired a great share of tools and financial support from states inciting terrorism. After increased pressure against the above states on behalf of the international community, financial and other support was severely mitigated, and some financing sources were shut down indefinitely. Moreover, new independent terrorist organizations acting at their own discretion have no access to foreign financing sources, as in case with traditional terrorist organizations. Due to the above, numerous terrorist groups are forced to use alternative financing sources, including funds acquired from illicit proceeds such as illicit trade in arms, kidnapping for ransom, extortion (racket) and drug trafficking.

The scales of illicit activities implemented by terrorists for own financing vary from petty fraud to grave organized crimes. Below are the types of illicit activities (including drug trafficking, cheque fraud and extortion) that were used by terrorists to raise required funds.

#### 3.4.1. Use of proceeds earned from drug trafficking in terrorism financing

Drug trafficking is a rather profitable source of money for terrorist groups, which allows raising substantial amounts. The rates of financing terrorist activities through trafficking in drugs have significantly increased after the amounts coming from states inciting terrorism dropped. This resulted in significant decrease of differences between terrorist groups and criminal organizations engaged in drug trafficking.

Both organized crime and terrorist groups keep expanding their international networks and concluding mutually profitable alliances. Globalization processes allowed criminal and terrorist organizations extending and diversifying their activities through the elimination of barriers in the field of telecommunications and communications, banking as well as open borders, all of which significantly simplified their operations.

Implemented investigations and acquired data allowed detecting close cooperation between various terrorist groups and criminal organizations engaged in drug trafficking. Such cooperation is caused by the necessity, convenience or mutual benefits.

Below are the examples of the above cooperation.

### Case Study 3.4.1.1. Trade of drugs for weapons

Nine persons took part in conspiracy to purchase weapons of the total value of **USD 25 million** in exchange for cocaine and cash.

The group leaders were eventually arrested during the preparation to check on a covert stash of weapons as a result of an operation involving law enforcement agents in one of Caribbean countries. A broker in arms deals was arrested during a simultaneous operation in a North American country.

The above scenario provides a chance to understand how a terrorist organization attempted to finance its operations (including purchase of arms) through trade in illicit substances. As a result of the investigation, seven suspects pleaded themselves guilty of material support to terrorists and conspiracy focused on drug trafficking. Three suspects only pleaded themselves guilty of conspiracy focused on material support to terrorists.

Law enforcement authorities are in the middle of a related investigation.

### Case Study 3.4.1.2. Extortion of funds from drug traffickers by a terrorist organization

During an investigation and judicial prosecution implemented by public administration of an Asian country regarding a terrorist organization, it was detected that drug trafficking was the major source of its proceeds. Narcotics were grown in Pakistan, Afghanistan and Iran and later trafficked to Europe while involving infamous members of the above organization, common militants and accomplices.

During the related investigation, more than 10 terrorist group members were arrested together with substantial amounts of money. As a result of investigative activities and acquired witnessing of arrested members, it was established that the organization was dealing with money extortion from drug traffickers at checkpoints in the north of Iraq by imposing "taxes" in the amount of 7% of the total trafficked goods value upon them. The group also extorted cash for each person or vehicle crossing their "customs points". One of the above "customs points" earned from **USD 20,000** to **USD 30,000** weekly.

## 3.4.2. Use of proceeds from credit card fraud in terrorism financing

There are many various ways to commit fraud with the use of someone else's credit cards. One of the simplest of the above is to purchase goods online or by phone. At the same time, credit cards data can be used for both financing of terrorism and other types of illicit activities.

It is worth mentioning that demand for credit card fraud created a separate type of illicit activities – illicit trade in stolen credit card data, including credit card account numbers, card holders' personal information (complete personal data, phone numbers, validity periods, CVV codes, etc.).

### Case Study 3.4.2.1. Financing of terrorism through credit card fraud

A group of persons of North American descent in the number of 20-30 people, together with their accomplices working in the field of trade and service provision, managed to collect data from almost 200 stolen bank cards.

The above persons further referred the acquired data from a European country where the cards were issued to two other European countries where their accomplices stole more than Euro 200,000 from them.

The stolen funds were used for financing of European cells of the Al Qaeda network.

Law enforcement authorities are in the middle of a related investigation.

The above example is a bright demonstration of terrorists who not only know but also use a chance to acquire substantial amounts of money through credit card fraud. They are also able to use sophisticated fraud schemes and methods to finance terrorism.

### 3.4.3. Use of proceeds from cheque fraud in terrorism financing

Several cases of use of the most popular fraud involving banks to raise funds for terrorism financing were detected. The most common ones of the above include opening new bank accounts through the use of forged documents under a fake name as well as fraud with payments for goods<sup>13</sup>.

In order to implement their illicit intentions in practice, fraudsters open accounts and accumulate cheque books. After the number of cheque books has become extremely big, they are used for purchase of goods at trade warehouses for the amounts non-exceeding ceiling values in need of verification whether the funds are available on a certain account. Then the goods are returned, and their value refunded in cash. Such activities can be implemented by organized groups of persons who can sign cheques simultaneously for the same amount at various locations. Such a fraud allows terrorists raise and move substantial amounts of cash.

### 3.4.4. Use of proceeds from extortion in terrorism financing

Persons providing assistance to terrorist and militarized groups use their influence on communities and expatriates to seize their proceeds and savings. By demanding funds for their own needs, terrorists use various ways to threaten people in order to prevent any interference from law enforcement authorities. According to international and Ukrainian experience, extortion may be a substantial and stable source of funds for terrorist groups<sup>14</sup>.

#### Case Study 3.4.4.1. Use of extortion for terrorism financing

An ISIL cell has been detected and eliminated in Ukraine (committing illicit activities on the territory of Kyiv, Lviv, Kharkiv and Odesa Oblasts). The members of the above group committed extortions, armed robberies and other crimes to finance terrorism. They also provided support to ISIL members and followers in their attempts to infiltrate the territory of Ukraine.

During a related investigation, there was documented the fact of illicit proceeds in the amount of **UAH 200,000** by the members of the above organization. Firearms and munitions have been seized.

Six persons have been charged and detained for facilitating the operations of the above terrorist cell, and two persons were put on the wanted list.

The investigation is underway at the moment.

<sup>13</sup> "Terrorist Financing" FATF typology study, 2008, Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>

<sup>14</sup> "Terrorist Financing" FATF typology study, 2008, Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>



### 3.4.5. Use of various sourced illicit proceeds for terrorism financing

In order to raise funds required for terrorist operations, organizers can use any type of offences to earn profit while easily switching from one type of crime to another. Hence, one of the groups committed such crimes as burglary, personal data theft and credit card fraud to raise the required funds.

#### Case Study 3.4.5.1. Illicit proceeds used for terrorism financing

An individual financing terrorists was a member of a criminal organization whose leaders organized a tobacco product contraband scheme to USA. The above individual bought cigarettes in one of the states with low tax rates for tobacco products, marked the latter with forged excise stamps and imported them to another state as contraband (where the "cigarette tax" was significantly higher) without paying any related tax for further resale.

Moreover, the above organization produced forged credit cards, robbed retail and wholesale companies. The cash acquired as a result of the above activities was laundered through the purchase of companies, additional batches of tobacco products and additional credit card forgery.

The above organization also committed insurance fraud through the arson of their own cigarette store located in an Indian reservation to acquire insurance proceeds in accordance with an arson insurance contract.

An individual financing terrorists used profits acquired from the above criminal activities to provide material assistance for a terrorist organization.

A law enforcement authority is in the middle of a related investigation.

### 3.5. Movement of funds to finance terrorism

As well known, terrorism requires constant financing, and the amounts of funds involved in support to terrorism are enormous. Quite often, countries (regions or territories) hosting fundraising operations are at some distance from the regions of terrorist activities, which is the basis to move raised funds directly to terrorists.

There are three basic methods used by terrorists to move funds. The first one considers the use of a related financial system, the second method is physical movement of funds (e. g., through the use of cash couriers or so called "mules"), and the third method is based on the use of international trade. Terrorist organizations also apply alternative systems of money transfers, charitable or other organizations under their control.

The variety of organizational structures used by terrorist organizations, constant adaptation to current and emerging methods and means to counter terrorism financing applied by international society as well as high terrorists' fitness to external changes does not allow defining the most common way for movement of financial assets. Normal operations of a certain terrorist group can be most easily ensured through traditional banking systems since money transferred from one country to another one can be easily hidden through the use of accounts opened under fake names, charitable organizations or companies that allow masking the actual recipient. However, there are cases when other methods are used to move funds, including those to hide any tracks of terrorists' financial activities.

In many cases, methods used by terrorists for raising, moving or using financial assets required for terrorist financing activities can be very sophisticated, and their operations can be practically equivalent to common business (financial) activities.

The experience earned due to implemented investigations proves that none of the methods and ways used to move funds between different countries can be considered absolutely safe. Hence, all of them has a certain risk level and can be used by for terrorism financing. This claim is based on a common feature of basic (most commonly known) ways to transfer or move money: in case a terrorist activity is implemented in a location which is different from the country of funds' origin, interrelations between the source of money and terrorism are very difficult to detect.

### 3.5.1. Use of a state financial system in terrorism financing

Banking institutions, non-banking credit-financial facilities and other establishments providing financial services form the financial state sector are intermediaries ensuring functionality of state economy by their nature.

One of the basic activity types for the above institutions is money transfers through international money transfer systems and their own payment systems as well as small alternative money transfer networks. The speed and convenience of financial transactions as well as their great number form prerequisites for increased risks of using a legal state financial system for terrorism financing.

The use of legal financial intermediaries together with economic agents of non-transparent property structure (e. g., offshore companies) provides an opportunity for terrorists to mask their operations and launder their illicit gains.

Investigation into a number of terrorist attacks allowed establishing that radical groups and persons linked to terrorist organizations used a network of legal money transfer companies working all over the world to transfer and receive funds. Compliance with the requirements set by FAFT Recommendation 16 of 2012 allowed implementing an efficient analysis of the above operations, which gave better understanding on the circle of terrorists' contacts and defining networks used for terrorism financing.

Development of money transfer technologies and payment systems provides a two-sided impact in the sense of illicit use of the above systems by persons financing terrorism as well as those laundering their money.

On the one hand, electronic payment systems expand the capacity of law enforcement authorities in tracking specific transactions while using the data automatically generated, stored and/or transferred during money transfers.

On the other one, new technologies become attractive for use by potential terrorists. Hence, increased speeds and volumes of money transfers combined with non-compliance with international standards against financing of terrorism, money laundering and WMD proliferation by participants of the above transfers result in complicated control over such transfers..

### Case Study 3.5.1.1. Use of international money transfer systems for movement of funds by terrorist organizations

---

It was detected that a terrorist organization from the **Country X** transferred money (used for rent of safe houses, trade in vehicles, purchase of electronic components for explosive devices, etc.) to the **Country S**. Related accounts in both countries were opened for individuals not connected to any terrorist organizations but in family relations with terrorists. Therefore, those were the family relations that could be used as a rationale for money transfers when necessary.

Monetary assets (mostly in the format of cash deposits) were deposited by a terrorist organization to the above banking accounts and further used for money transfers. After receipt of money in a point of destination, an account holder either let them be or invested those into equity funds to be kept there until required. The money could be also transferred to another bank account managed by a financial manager working for the terrorists and used for purchasing equipment, materials and other accidentals of the terrorist organization during its operations.

A law enforcement authority is in the middle of a related investigation.

Together with international payment systems, terrorists also often use national payment systems to meet their needs.

### Case Study 3.5.1.2. Use of national money transfer systems for terrorism financing

---

A criminal group was eliminated on the territory of Kyiv Oblast. The above group was related, among other things, to financing of terrorist operations of illegal armed groups in ORDLO.

Citizens of Ukraine – the suspects of a related proceeding – registered companies for use of their details to conclude contracts with companies implementing economic activities on the temporary occupied territories of Lugansk Oblast as well as fictitious sale-purchase or service provision agreements.

In their own term, the above companies implementing economic activities on the temporary occupied territories of Lugansk Oblast transferred monetary assets to bank accounts of commercial facilities in the city of Kyiv in accordance with the above fictitious documents. The money was further transferred to suspects' bank accounts as well as to accounts of other individuals engaged in illicit activities (30 persons have been identified so far).

The above funds were later withdrawn in cash through ATMs and offices of Ukrainian and Russian banks and moved to the occupied territories of Lugansk Oblast.

During the cashless-to-cash conversion operation, the suspected criminals were detained.

Monetary assets in the amount of approximately **UAH 1** million, fictitious documents, forged company stamps and seals as well as firearms and ammunition were detected and seized during the investigation.

The case is now being examined by the court.

### Case Study 3.5.1.3. Use of a national financial system in terrorism financing

Illicit activities of individuals aimed at terrorism financing have been ceased.

In accordance with the acquired information, a group of individuals implemented currency exchange operations on the ORDLO territory as well as transfers to/from their personal accounts through internet-acquiring after having opened accounts at Ukrainian banking institutions. The acquired funds were later moved to support activities of terrorist groups on the ORDLO territory.

The above group is suspected of committing a criminal offence in accordance with Part 3 Article 258<sup>5</sup> of the Criminal Code of Ukraine.

The investigation is underway at the moment.

### 3.5.2. Use of trade in terrorism financing

Due to its diversity and dispersion, the system of international trade contains a great number of risks and myriads of vulnerabilities allowing terrorists to transfer funds for goods on rather legal terms and conditions<sup>15</sup>.

According to a FATF study, money laundering in the field of trade is an important channel for organized crime. Considering the ever-growing rates in international trade, it poses an increasing FT risk.

The ways to launder money in the field of trade differ by their complexity. The most of basic schemes include common fraud practice considering, among other things, overstated or understated value of goods or services within invoices. However, more complicated schemes combine fraud methods of money transfers with the use of a state financial system (as cheques or bank transfers) and physical movement of cash (through cash couriers). Such comprehensive transactions complicate tracking and detection operations for moved values.

#### Case Study 3.5.2.1. Movement of funds by terrorists with the use of trade

Officers of a foreign FIU acquired information from several banks on certain account holders – the **Individual A**, **Individual B** and **Company C** implementing trade operations in diamonds. During several months, the accounts of the **Individual A**, **Individual B** and **Company C** were used for substantial money transfers and receipt of substantial amounts of money from other countries. Moreover, the **Individual B** acquired several bank cheques for substantial USD amounts soon after opening an account.

The information collected by the FIU officers proved that the **Company C** received substantial USD money transfers from companies dealing with diamond-related activities. As soon as the **Company C** received a money transfer, it broke it down to several smaller ones and referred them to the **Individual A**, a European citizen born in Africa and residing in the Middle East.

One of the **Company C**'s directors, a citizen of the **European Country B**, residing in Africa had a bank account in the **European Country B**. the above account was used for money transfers to/

<sup>15</sup> "Terrorist Financing" FATF typology study, 2008, Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>



from European, North American and Middle Eastern countries. The most of incoming transfers were in USD, later converted to Euro and transferred to other countries. Among other things, the above transfers were made to accounts in the **European Country B** held by the **Individual B** and his wife.

In accordance with personal information and data acquired from the FIU, a case was opened regarding diamond trafficking from Africa. The most substantial amounts of money from the company trading in diamonds was transferred to the **Individual A** residing in the Middle East. In accordance with available information, it was known that both the **Individual A** and **Individual B** were suspected of procuring diamonds from a rebel army active in one of the African countries and trafficking of the above diamonds to Belgium for one of terrorist organizations.

Moreover, it was established that FIU officers had previously referred this information on specific persons and companies related to the **Individual A** and **Individual B** regarding their connections in other cases of money laundering.

A law enforcement authority is in the middle of a related investigation.

### Case Study 3.5.2.2. Use of trade in terrorism financing

In accordance with the analysis of financial transactions and additionally acquired information, there was detected a scheme dealing with suspicions of FT through the procurement of components and other goods that could be used for production of specialized technical devices and further sold for the benefit of illegal armed groups in ORDLO.

It was established that the **Company A** received money, mostly from public administrations and charitable organizations, as a payment for goods (peripherals, specialized equipment) and charity aid for the total amount of **UAH 226 million**.

Moreover, officials of the **Company A** deposited funds in the amount of UAH 6 million to the company's accounts (including those detailed as trade receipts in the amount of UAH 3 million) suspected of being received from sale of specialized technical equipment manufactured within the company's premises and handed for the benefit of ORDLO illegal armed groups for a monetary reward.

The funds further accumulated at the **Company A's** accounts were transferred to procurement of other components and goods that could be used for production of specialized technical equipment for the benefit of 200 economic agents in the total amount of **UAH 84 million** and 116 individuals-entrepreneurs in the total amount of **UAH 28 million**.

A part of the above funds in the amount of **UAH 24 million** was transferred as a payment for labours for the benefit of the controlled **Company B**, which, in its own turn, transferred the above funds monthly for the benefit of the **Individual -Entrepreneur L** and **Individual-Entrepreneur M** as a payment for programming services.

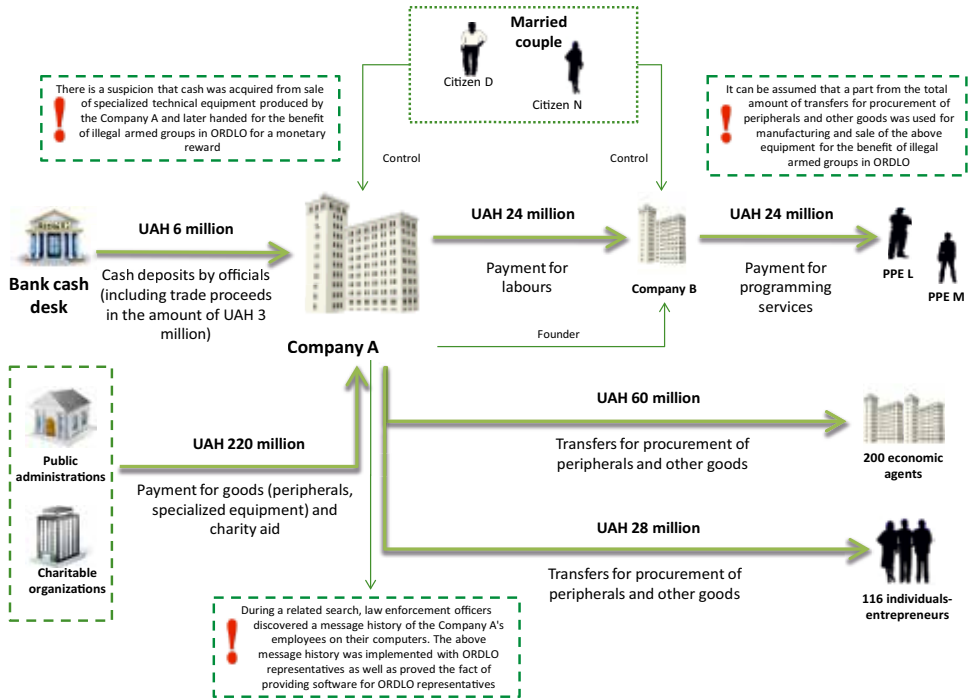
It is worth mentioning that a married couple of the **Citizen D** and **Citizen N** are the founders of the **Company A**. In their own turn, the **Company A** and **Citizen N** are the founders of the **Company B**.

During a related search, law enforcement officers discovered a message history of the **Company A's** employees on their computers. The above message history was implemented with ORDLO representatives as well as proved the fact of providing software for ORDLO representatives.

It can be assumed that a part of monetary assets from the total amount of transfers for procurement of peripherals and other goods, which could be used for manufacturing specialized technical equipment,

was used for manufacturing and sale of the above equipment for the benefit of illegal armed groups in ORDLO.

A law enforcement authority is in the middle of a related investigation.



### 3.5.3. Use of payment systems in terrorism financing

According to implemented investigations into terrorism financing, there are many methods used by individuals related to terrorist activities to raise/transfer funds, such as payments with the use of web-based technologies, electronic payment systems, money transfer systems or other alternative ways of remote access rendering full identification of a fund sender/recipient impossible as well as social networks.

In countries with weak banking systems and armed conflicts waging on their territories or those inciting activities of terrorist groups, money transfer operators can be used as major sources of money transfer/receipt.

One of the major risks related to terrorism financing for payment system operators is the lack of sufficient regulation and control over their activities, especially in terms of AML/CFT.

Immigrants and their families are significantly dependant on payment system operators when sending money to their homelands. This provides an opportunity to mask transfers linked to terrorism financing amidst legal money transfers sent to migrants' families (communities). This also complicates the procedure to detect FT-related transfers in the major flow of transferred money.

Considering the information acquired during the study, the following payment systems can be specified as those which were most often used for terrorism and separatism financing (according to implemented investigations): MoneyGram, WesternUnion, KoronaPay, Yandex. Money and Money@mail.ru.

#### Case Study 3.5.3.1. Use of payment systems for terrorism financing

In accordance with an analysis implemented and information received from a financial intelligence unit of a foreign country, SFMS detected financial operations related to a citizen of Libya, the **Individual C** suspected of terrorism financing.

It has been established that the **Individual C** (a citizen of Libya), while using multi-currency accounts opened at several Ukrainian banks, implements financial transactions through international payment systems (MoneyGram and WesternUnion) to receive money from citizens of various countries in small amounts.

The above funds were subsequently referred to the **Non-Resident Individual A** (Belgium) and detailed as "aid".

SFMS acquired information from a foreign FIU stating that the **Non-Resident Individual A** was suspected of forging identification documents for foreign Syrian fighters of terrorist groups and persons from Iraq to enter and stay on the territory of the European Union.

A related reporting entity and SFMS cancelled money withdrawal transactions for the **Individual C** (Libya).

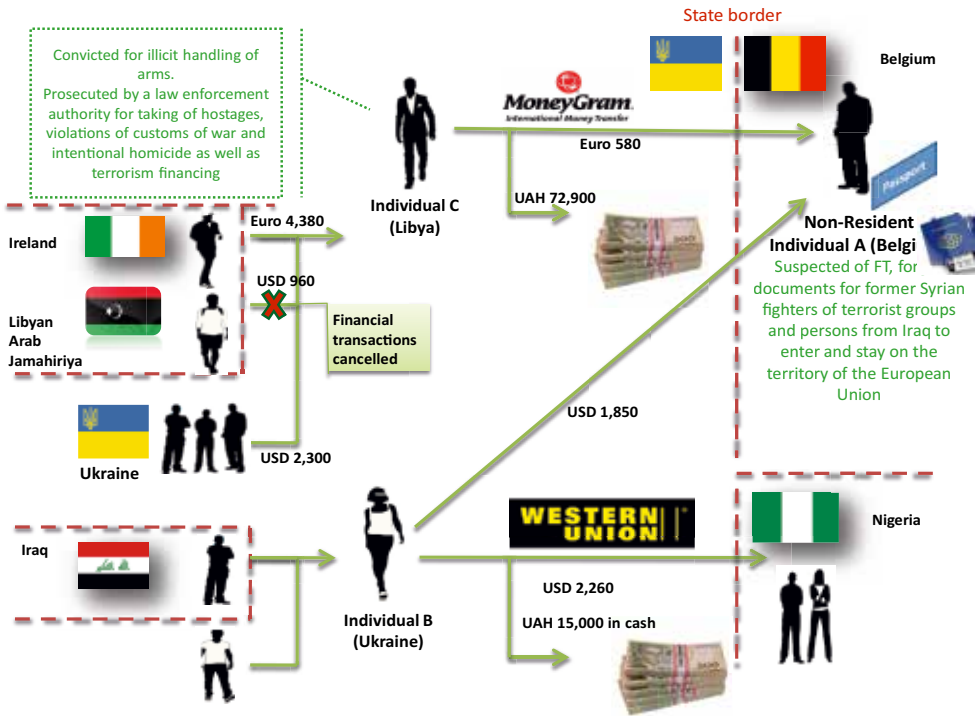
It was additionally established that the **Non-Resident Individual A** is connected to the **Individual B** (Ukraine) by financial transactions. There were no data on income declared by the **Individual B**. It was also established that the above person was registered on a temporarily occupied territory not controlled by the Government of Ukraine as of now. The **Individual B** implemented a money transfer

for the benefit of 3 individuals (destination country – Nigeria) and received funds from 1 individual (origin country – Iraq). No data on income declared by the **Individual B** are available.

The **Individual C** (Libya) is a suspect in several criminal proceedings under the following articles of the Criminal Code of Ukraine:

- Part 1, Article 263 “Illicit handling of arms, ammunition or explosive substances”. A court convicted the individual to 3 years of detention. In accordance with Article 75 “Release on probation” of the Criminal Code of Ukraine, the individual was later released after 1 year of detention;
- Part 2, Article 147 “Taking of hostages”;
- Part 2, Article 258<sup>1</sup> “Alluring to committing a terrorist attack”;
- Part 2, Article 438 “Violation of laws and customs of war”;
- Part 2, Article 258<sup>5</sup> “Financing of terrorism”.

A law enforcement authority has initiated a related criminal proceeding.



### Case Study 3.5.3.2. Use of payment systems to organize operations of a terrorist group

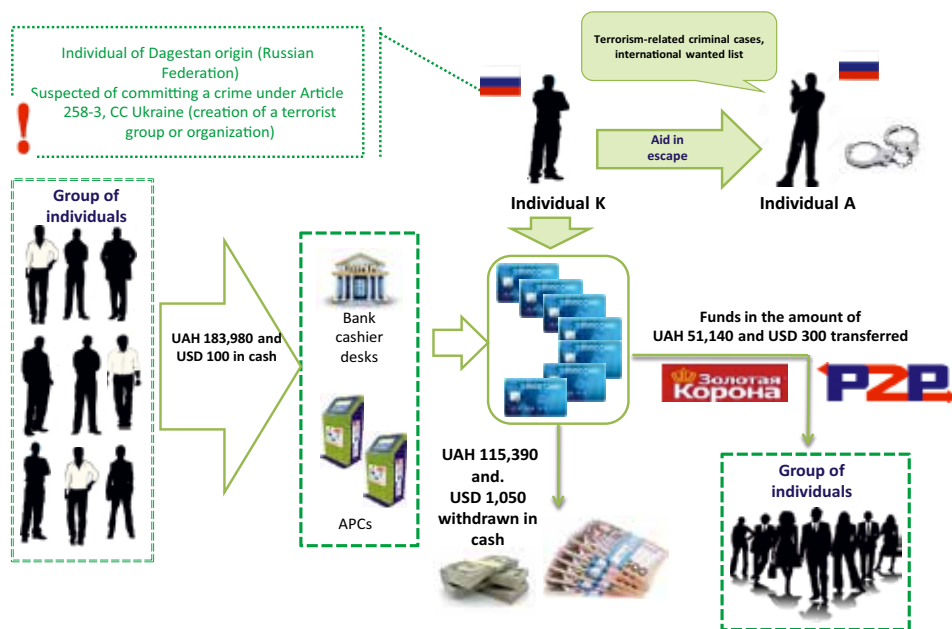
In accordance with an analysis implemented, it was detected that the **Individual K**, a citizen of a neighbouring state, had cash deposited and money transfers received on accounts in a Ukrainian bank in 2013-2017 on the regular basis. A part of transfers was later withdrawn in cash, and the rest of money was transferred for the benefit of various individuals.

In May 2015, as a result of an operation implemented by law enforcement authorities of a foreign country related to counteraction to ISIL, a citizen of the neighbouring state, the **Individual A**, was detained. Afterwards, the **Individual K**, together with other citizens of the neighbouring state, started raising funds to liberate the detained person and further transfer to Ukraine for participation in terrorist activities.

In June 2015, the **Individual A** escaped from custody by obtaining guards' weapons. However, in August 2015, the person was arrested in the city of Kyiv by officers of the Security Service of Ukraine. Other citizens of the neighbouring state were found at the place of the **Individual A's** residence.

It was established that the above individuals were suspects in criminal cases in the neighbouring state related to terrorist activities and put on the international wanted list. Moreover, one of the detained was on the list of organizations and individuals related to extremist activities or terrorism.

A law enforcement authority is in the middle of a related investigation.





**Case Study 3.5.3.3. Use of an electronic payment system for terrorism financing**

In accordance with an analysis implemented, a scheme of financial transactions was detected with presumed relation to terrorism financing through the use of an electronic payment system.

According to a financial investigation, it was established that the **Company A**, being the owner of a national non-banking payment system, maintains payment terminals located in ORDLO.

It was also established that the **Company A**'s dealers maintaining operations of self-servicing software-hardware sets (payment terminals of the national non-banking payment system on the temporarily occupied territories) were the companies registered by the so called "Ministry of Income and Fees of ORDLO" paying taxes to the budget of a terrorist organization on the ORDLO territory.

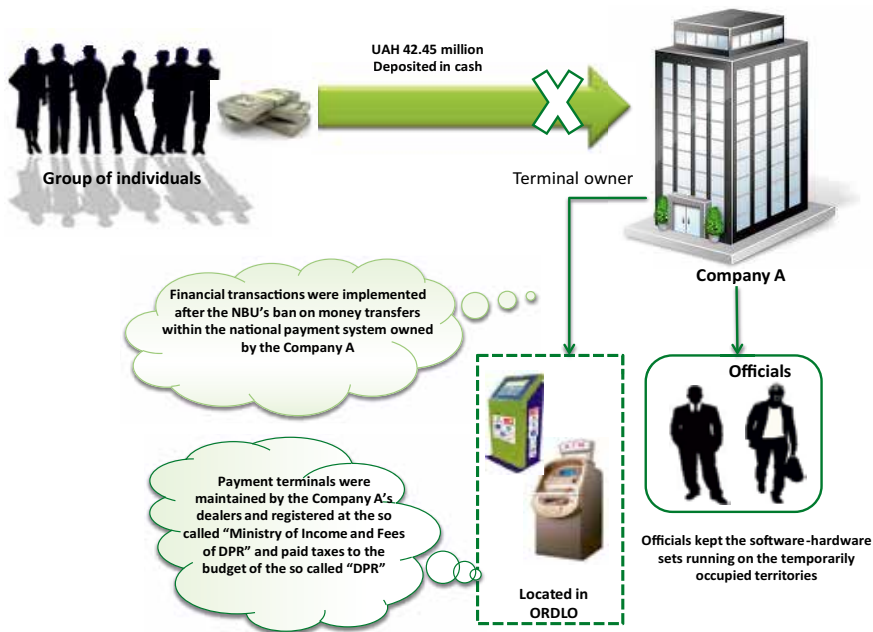
With the above facts in mind, money transfers within the national payment system owned by the **Company A** were suspended.

At the same time, ignoring the ban on transactions through payment terminals located on the non-controlled territory, cash was deposited.

It was also established that a **group of individuals** deposited **UAH 42.45 million** in cash to the **Company A**.

SFMS has made a decision on suspending the above financial transactions.

A law enforcement authority is in the middle of a related investigation.



#### Case Study 3.5.3.4. Use of national payment systems for terrorism financing

A criminal group related to terrorist financing activities committed by illegal armed groups on the temporarily occupied territory of Lugansk Oblast was eliminated in Kharkiv Oblast.

The **Citizen of Ukraine B**, a suspect of a proceeding under a case of financing of illegal armed groups in ORDLO, opened card accounts for figureheads or controlled persons at the **PJSC P** in the city of Kharkiv.

The above accounts were further used to receive funds from the territory of Ukraine and a neighbouring country.

The received funds were withdrawn in cash at ATMs of Kharkiv city and physically moved by the **Citizen B** to the temporarily occupied territory of Lugansk Oblast with further terrorist financing activities as well as payment of wages for members of illegal armed groups on the ORDLO territory.

**UAH 34.1 million** were received to the **PJSC P** in total for the whole period of the above illicit scheme being active, of which **UAH 27.2 million** were received in cash.

According to a related court decision, the **Citizen B** was found guilty in committing a crime under Part 2 Article 258<sup>5</sup> of the Criminal Code of Ukraine and convicted to a penalty harmonized by the parties under Article 69 of the Criminal Code of Ukraine as well as a fine in the amount of 20,000 tax-free minimum incomes of an individual (**UAH 340,000**) with confiscation of property, including monetary assets in the amount of **UAH 86,400**.

The **Citizen B** remained in custody and keeps serving his sentence.

#### 3.5.4. Use of cash transporters (cash couriers) for terrorism financing

Physical movement of cash is one of the methods used by terrorists to move funds outside the rule of law regulating credit and financial institutions and preventing money laundering and terrorism financing. At the same time, certain groups could withdraw their assets from the financial system in order to avoid control by exchanging cash into gold or precious stones<sup>16</sup>.

Physical transborder movement of cash is widely popular in the countries wherein the electronic banking system is at the initial stage of its development or almost out of use by common citizens. Economies of numerous nations in Africa and Middle East as well as post-soviet countries are based on the use of cash, which forms natural benefits for its movement through alternative transfer systems or cash couriers. Investigations in a number of terrorist attacks demonstrated that cash couriers are used even in the countries with highly developed financial systems. In most cases, such transporters are dealing with movement of cash earned outside of a related financial system.

Due to the fact the majority of credit and financial institutions strengthen their means in proper client verification, such a method of monetary asset which leaves no tracks for possible verification is getting more and more demand for. In case cash is intercepted during a transborder operation, it can be very complicated to track its origin and destination. Low volumes of cash moved in such a way are yet another barrier to detect and intercept movements as such.

<sup>16</sup> "Terrorist Financing" FATF typology study, 2008, Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>

### 3.6. Emerging terrorist risks

Ways and methods to finance terrorist activities develop and improve while basing on advanced technologies or intended attempts to bypass the measures taken by law enforcement and other competent authorities and agencies to counteract terrorism financing. The risk of using emerging systems for terrorism financing is rather high and keeps growing. This deals with the expanded scales of the use for the above systems. Many of those are available all over the world and used for fast money transfers. Moreover, a number of online money transfers or digital currencies ensure anonymity by their nature, which makes them attractive for terrorism financing. This is of even higher relevance in case the head office of a payment system is located in a country with a rather weak AML/CFT.

As mentioned above, terrorists and terrorist organizations are fast with adapting to changes and use new financing methods for their terrorist operations.

Social networks, new payment products and services as well as the use of natural resources are the new fields to study in the context of FT counteraction. This section provides a general overview of emerging ways and methods to finance terrorist activities in accordance with the methodology proposed within the FATF typology study.

#### 3.6.1. Fundraising with the use of social networks in terrorism financing

Wide Internet access and anonymity with the fast expansion of social networks are used by terrorist groups to raise funds from their followers all over the world, which poses a threat to preventive activities aimed against terrorism financing. Terrorist organizations widely use social networks and worldwide web to promote terrorist ideas and build contacts with their followers<sup>17</sup>.

Social networks can be used in fundraising to simplify money transfers as well as facilitate to exchange in numbers of credit cards, prepaid card details as well as identification information on bank accounts.

Social networks are also used in coordination of fundraising efforts. Wide-scale and well-organized fundraising schemes for terrorism financing may involve up to several thousands of “backers”, hence operating substantial amounts of money. Today terrorist organizations can implement their information and propaganda activities in a huge audience while using communications initiated in chats or message boards and continued in social networks. Such communications are sometimes supported by mobile device applications.

Fundraising or crowdfunding to support terrorism and extremism is implemented under the mask of legal charity or humanitarian aid. Sometimes even charitable organizations are established for that reason. Funds can be raised in secret or under the cover of humanitarian aid. Persons donating money often have no idea of the final purpose for the funds raised.

<sup>17</sup> “Emerging Terrorist Financing Risks” FATF typology study. Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>

As a rule, crowdfunding announcements are posted in social networks, issue-related websites, specialized networks and closed message boards on the web as well as sent out in private messages. In order to mask actual purpose of fundraising and avoid blocking, such announcements often have no direct indicators that the funds are crowded for terrorism financing. Instead they use masked statements or indicate that money is raised for presumably charitable or humanitarian needs. Fundraising announcements and details can be posted not in the textual format but, for instance, as an image or video. This renders detection of such announcement through standard search engines impossible as well as complicates the detection of websites posting the above announcements. Moreover, this complicates search for the above announcements through the known details.

Movement of raised funds is implemented in several stages: raised money is sent as a series of electronic transfers; then it is withdrawn in cash for further movement by cash couriers. Sometimes cash is deposited to other accounts. Such schemes are aimed at destroying the link and masking the source of money or final recipients.

### Case Study 3.6.1.1. Crowdfunding in social networks

---

A financial operation scheme involving the **NGO O** was detected. The above organization was established and aimed at direct collection of money to support individuals suspected of mass rioting in Kharkiv and Odesa oblasts in 2014.

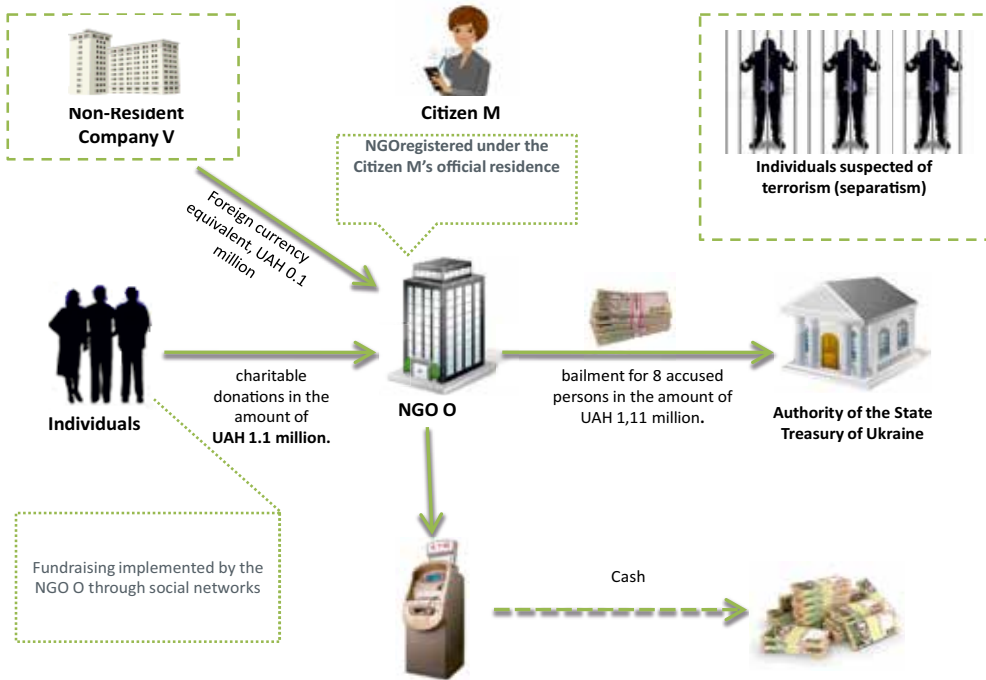
In 2015, the **Citizen M** registered the **NGO O** at her personal address. The above organization collected money from individuals and legal entities through social networks to raise funds for support of individuals detained at penal institutions and suspected of crimes against national security.

During 2016, the **NGO O** received charitable donations from individuals to its bank accounts in the amount of **UAH 1.1 million** and **UAH equivalent 0.1 million** in foreign currencies.

Further, the **NGO O** transferred a part of the above funds as bails for suspects detained by law enforcement authorities for crimes committed.

The remaining funds were withdrawn in cash by the **Citizen M** from the bank accounts of the **NGO O**. As a result, debit transactions under the account held by the **NGO O** were suspended.

A law enforcement authority is in the middle of a related investigation.



### 3.6.2. Use of virtual currencies in terrorism financing

Emergence of virtual and digital currencies facilitated fundraising in substantial amounts by involving the payment mechanisms designed for providing a newer, faster and more convenient way to transfer money through the use of internet. At the same time, payment products and services based on virtual currencies pose risks of money laundering and terrorism financing<sup>18</sup>.

#### For reference

*Virtual currency is a demonstration of value that can be traded digitally and operates as an exchange medium, monetary unit of account and/or store of value, but its legal payment status is not clearly defined internationally and significantly differs between various countries.*

*In some nations, virtual currencies still have no official status and are not an officially valid or legal way of payment for creditors.*

*Virtual currencies are neither emitted nor ensured by any jurisdiction while implementing the above functions only on consent of a community run by virtual currency users. Virtual currency is different from fiat currencies (national currencies) which are a legal way of payment, circulation and common use as well as an exchange medium and accepted within a certain emitting country.*

<sup>18</sup> . "Emerging Terrorist Financing Risks" FATF typology study. Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>



*Virtual currencies are also different from electronic money since the latter are a digital method to express a fiat currency and used for electronic transfers of value (demonstrated) of a fiat currency.*

*Electronic money is an electronic method of digital transfers for fiat currencies. Hence, it is used for electronic money transfers and has a legal payment instrument status.*

On the one hand, cryptocurrencies such as Bitcoins open new opportunities for innovations within the financial sector. However, they also draw attention of various criminal groups and may pose FT-related risks. This technology allows implementing anonymous money transfers internationally. Despite the fact of outgoing currency purchase may be identified (e. g., within a banking system), it is difficult to detect subsequent transfers of virtual currencies. The recent studies prove that criminals search and find virtual currencies that can ensure anonymity for both users and transactions, allow for fast transfers of illicit proceeds from one country to another one, widely used in the criminal world and have demand for.

### **Case Study 3.6.2.1. Use of virtual currencies for terrorism financing**

---

On 28.08.2015, Ali Shukri Amin was sentenced to 11 years in prison with further federal supervision for the rest of his life. This sentence was delivered for his web activities aimed at providing material support and resources to ISIL.

On 11.06.2015, Amin pleaded himself guilty of using Twitter for consulting and promotion of ISIL and its followers. Amin instructed on how to use Bitcoins for masking financial flows run by the Islamic State as well as consulted ISIL followers willing to travel to Syria to join armed action in the ranks of ISIL. Amin also confirmed that he facilitated a teenager from Virginia who had decided to go to Syria in 2015 and join ISIL. On 10.06.2015, the above teenager was charged with conspiracy in order to provide financial support to terrorists, conspiracy to provide material support to ISIL as well as conspiracy to commit murders and injure citizens abroad in the eastern district of Virginia.

Amin's Twitter account was visited by more than 4,000 followers, and he posted more than 7,000 tweets to support ISIL. Specifically, Amin used the account to discuss ways of financial support to ISIL via Tweeter with the use of Bitcoins and ways to establish a secure donation and financing system for ISIL.

For instance, Amin tweeted a link to his own article titled "Bitcoin wa 'Sadaqat al-Jihad" ("Bitcoins and charity for jihad). The above work contained ways to use Bitcoins for jihadists for financing of their activities. The article also provided clarifications on the nature of Bitcoins, the way this virtual currency system operates as well as suggestions to use a new Bitcoin Wallet, Dark Wallet, ensuring anonymity for Bitcoin users.

Moreover, the article also contained guidelines on the algorithm to create an anonymous donation system with the use of Bitcoins for sending money to mujahids.

A law enforcement authority is in the middle of a related investigation.

### 3.6.3. Use of prepaid cards for terrorism financing

Prepaid cards are cards with directly written or remotely stored data containing a certain amount of electronic money or its value. Despite the big variety of prepaid cards, the biggest risk to use prepaid cards for terrorism financing is posed by those cards which are emitted by systems that allow withdrawing funds through ATMs all over the world<sup>19</sup>.

Prepaid cards emerge to replace travel cheques as means to move funds abroad. Due to their specifics, such cards are in high demand for terrorism financing since they can be replenished in the country of origin with cash or electronically without any reporting and then secretly moved abroad without any declaration of their transborder movement. Afterwards, as soon as such a card enters a country with high risk of money laundering and terrorism financing or a fund-transiting state for money purposed for terrorism financing, funds are withdrawn in cash at ATMs located in such countries. The only restriction for such transactions is the single cash withdrawal through an ATM. As soon as a card is abroad, the funds deposited thereto become available for terrorists or their followers with minimum risks of identification when withdrawing money.

Prepaid card providers with the set ceiling values non-exceeding related AML/CFT restrictions are not covered with requirements to proper client verification. Such requirements to providers complicate identification of an individual who purchases a prepaid card. Moreover, some of these systems consider an opportunity to manage the same amount of money with the use of several cards simultaneously. For example, some other individual can deposit money with one card, and foreign recipients may access these funds abroad through another “linked” card. Moreover, any individual can access funds stored at such cards through a PIN-code provided when purchasing the card itself. This allows sending cards to third parties simpler and safer than moving cash in person. Finally, some prepaid cards provide an opportunity of direct transfers between individuals without any providers involved.

<sup>19</sup> “Emerging Terrorist Financing Risks” FATF typology study. Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>

### 3.6.4. Use of revenues from the exploitation of natural resources and mineral deposits for terrorism financing

Exploitation of natural resources is one of the methods used by terrorist organizations to control and hold territories as well as ensure their financing through criminal activities and possible connections to organized crime. Such a criminal activity includes extortion, contraband, looting, illicit mining, kidnapping for ransom, corruption and ecological crimes<sup>20</sup>.

In the countries with no efficient control of law enforcement authorities over specific territories, natural resources located thereat can be used for terrorism financing. Terrorists may use such resources to acquire funds through control or exploitation of natural resources such as oil, gas, coal, timber, diamonds, gold and other precious metals, fauna (e. g., trade in ivory). Use of natural resources and mineral deposits can be a reliable source for terrorism financing, and their attractiveness for terrorists is based on weak regulation of their mining on non-controlled territories. Moreover, terrorism financing at the cost of natural resources is actively practiced in the regions with a historically weak institutional basis, current political instability or armed conflicts as well as regions rich in natural resources. This initially refers to West Africa, some regions in South America and, as of 2014, temporarily occupied territories of Donetsk and Lugansk Oblasts.

The companies dealing with mining of mineral deposits often face extortion from terrorist organizations for the right to work in specific regions or territories. Such companies also tend to face a risk of extortion and kidnapping of their employees for ransom.

Financial sources may include extortions from farmers and agricultural producers as well as mining and refining enterprises. Hence, the illicit "coal" tax with the amount as high as up to 30% of the coal value, illicit trade and "taxation" at checkpoints and ports for shipment and transshipment of charcoal is considered the main source of financing for the Al-Shabaab terrorist group. These proceeds constitute from USD 38 million to USD 56 million according to different assessments.

<sup>20</sup> "Emerging Terrorist Financing Risks" FATF typology study. Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>

**Case Study 3.6.4.1. Use of revenues from the exploitation of natural resources and mineral deposits for terrorism financing**

In accordance with an analysis implemented, a scheme of financial transactions was detected. The above transactions deal with accumulation of funds at a legal entity’s account. This entity is located on the temporarily occupied territory of Ukraine. There was an attempt to transfer the above funds and possibly use those for terrorist financing activities in the future.

It is known that **LLC S** located on the temporarily occupied territory of Ukraine implements exporting operations of coal mined by several enterprises also located on the ORDLO territory for the benefit of the **Non-Resident Company V**.

The **Non-Resident Company V** paid **LLC S** for the exported coal in the amount of **USD 2.1 million (UAH 51.4 million)**.

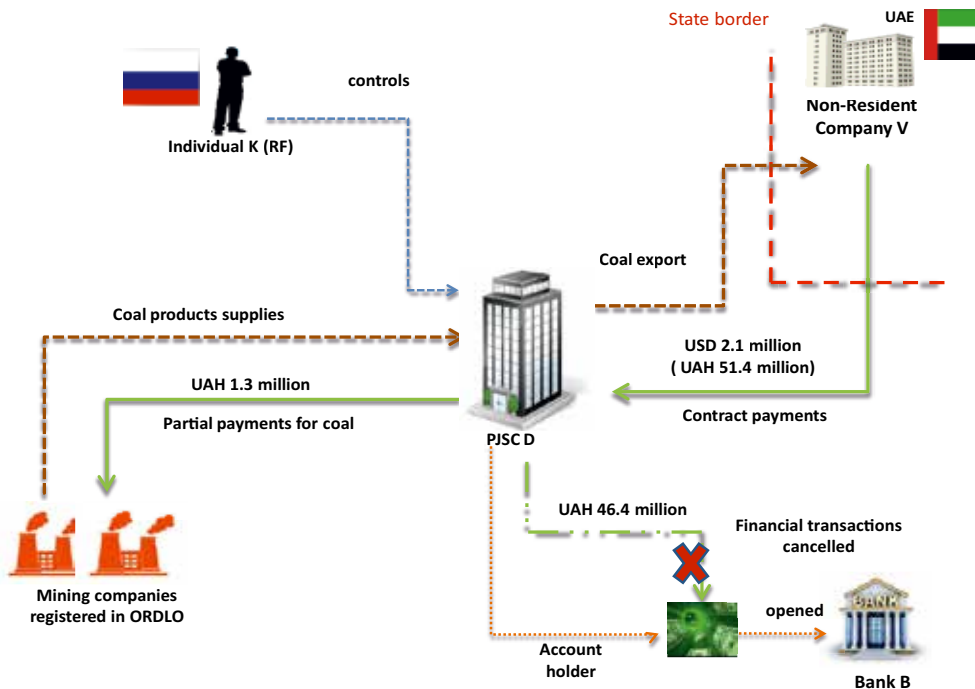
A part of the received funds in the amount of **UAH 1.2 million** was later transferred by **LLC S** for the benefit of mining companies (located in ORDLO) for the coal supplied.

Another part of money in the amount of **UAH 46.4 million** was transferred by **LLC S** to its other personal account.

A related reporting entity and SFMS made a decision on cancelling the above transactions.

It is known that **LLC S** is controlled by the **Citizen K** of Russian citizenship.

A law enforcement authority is in the middle of a related investigation.



### 3.6.5. Use of the oil and gas industry for terrorism financing

The use of the oil and gas industry for terrorism financing is mostly related to operations of the ISIL international terrorist group. The report on the “Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)” FATF typology study provides that ISIL strives to manage the local oil infrastructure to recover and refine oil for both their personal needs and sale or exchange at local and regional markets at a low price. The biggest proceeds are earned by ISIL from the use of produced oil and oil products or their sale to local buyers. Another part of income is earned by ISIL from trade in oil through intermediaries and smugglers selling and transporting illicit oil (oil products) to end users. ISIL commonly earns proceeds from oil trade in cash, which complicates tracking and elimination of this illicit activity.

Illicit use of oil and gas also occurs in other regions of the world. For instance, approximately 10% of oil produced in Nigeria (wherein recovery rates constitute up to 2 million barrels daily) is looted through well-organized transnational illicit schemes involving criminal networks, corrupted officials and military. There is a high risk that income from such looting goes to terrorist and extremist groups such as the Movement for the Emancipation of the Niger Delta (MEND).

### 3.6.6. Use of the mining industry for terrorism financing

Mining companies often work in regions not controlled by governments at all or those within the grasp of corrupted officials. Sometimes these locations also concentrate a high number of terrorist groups. For example, in West Africa, such groups as Al-Qaeda in the Islamic Maghreb (AQIM) and Movement for Oneness and Jihad in West Africa (MOJWA) deal with control and extortions in return for the right to mine mineral deposits. They often pose no strict requirements to mining companies. Operators dealing with mining of mineral resources can be followers of terrorist organizations or contribute to activities of terrorist groups. There is a high risk that donations from legal and illegal mining entrepreneurs can be directly or indirectly referred to terrorists<sup>21</sup>.

Illicit gold mining is widely spread in the whole South America, but in Columbia, it is suspected of having relations to drug trafficking and armed attacks committed by terrorist groups such as Revolutionary Armed Forces of Colombia – People’s Army, also known as FARC. According to Columbian authorities, 87% of mining companies work outside the rule of law, and in a number of regions, this activity replaced cocaine trafficking while being implemented by such rebel groups as Choco, Caqueta and Amazonas.

21 “Emerging Terrorist Financing Risks” FATF typology study. Report. [Electronic resource]. Access mode: <http://www.fatf-gafi.org>



### 3.6.7. Use of informal payment systems for terrorism financing

Development of labour migration and international trade raise demand for services provided by payment systems, including alternative money transferring systems on the transnational level. At the same time, terrorist activities and operations of organized crime are also on the rise in the field of developing payment and money transfer schemes that allow bypassing control tools set by the state, especially in the AML/CFT. The use of alternative (informal) money transfer systems in money laundering and terrorism financing have become a global threat.

Hawala is the most popular alternative system with a long history and spread mostly in Islamic countries or territories mostly inhabited by Muslims such as Middle East, Africa and Asia. Hawala and similar services are popular among labour migrants and peddlers, but there are cases when systems as such are also used by criminal elements and terrorists.

According to current estimations, there are approximately 5,000 Hawala brokering points all over the world operating at big marketplaces. Related cashier desks work under cover of a small company – from wristwatch repairs to fruit sellers and others. Hawala uses short-lived firms to transfer money to legal bank accounts as well (as a rule, those in offshore areas).

A similar system is based on money transfers through one-time messages (e. g., email, fax or phone calls). Material values are moved from one country to another without any supporting financial documentation. Due to the fact that all the financial transactions are implemented through the netting method or at personal encounters, state controlling bodies are not able to track these financial flows.

In order to send money, a client approaches a system broker who sends a message to a partner in a destination country after receiving money (by email, fax, phone etc.). A message as such only contains the amount, recipient's name and code (most often, a line of digits on a banknote). In order to receive money, it is sufficient to name the code of a related payment. Settlements between brokers are implemented clearing-wise, including the use to cover the balance of counterfeit gold, precious metals, etc.

Hawala-like systems are considered very dangerous in many countries since these networks can be used by terrorists to transfer almost unlimited assets to any country. It is very problematic to track transfers under such systems or prove a person's allegation to illicit money transfers.

Hawala and other alternative systems can be very fast to deliver money due to a developed network all over the world. Internal relations for such systems are based on trust and settlement payments with close to none documentation managed. Hence, it can be very difficult to prove that a person is related to money laundering or terrorism financing.

The most typical specifications of systems similar to Hawala are as follows:

Despite recent improvements and strengthened AML/CFT tools, the risks related to the use of informal payment systems in illicit activities remain high. This mostly relates to their geographical and financial availability. In many countries with a heightened terrorist threat level, Hawala-like

systems have been traditional ways to transfer money, both legal and crime-related. Limited access to banks, high corruption rates and will to evade taxes make law-abiding citizens use non-registered informal systems on par with criminals.

Below are several case studies of using Hawala –like systems by terrorists.

#### Case Study 3.6.7.1. Terrorist abuse of Hawala-like systems: The Times Square Bombing case

---

The Manhattan Federal Court convicted Mohammad Younis for the implementation of illicit money transfers between USA and Pakistan without a proper license. One of the above transfers was used to finance a bombing attempt at Times Square in New York.

Mohammad Younis provided money transferring services for individual persons in the city of New York while using the methods natural for the Hawala system. While using informal systems, Younis implemented two separate transactions for the clients coming from Connecticut and New Jersey to meet him at Long Island. During each operation, Younis handed thousands of dollars in cash to individuals, as instructed by his accomplice in Pakistan, without knowing the final purpose of the above funds. Younis had no license to implement the above transactions (neither from the state nor from federal administrations).

One of the persons Younis handed money to was Shahzad, an organizer of a failed bombing attempt who was eventually convicted under ten criminal charges related to his attempt to blow a car bomb (VBIED) at Times Square. During the trial, Shahzad confirmed that he had acquired money in USA in April of the same year to prepare the terrorist attack. The money was sent from Pakistan by members of Tehrik-i-Taliban, a military extremist group that had trained him in handling with explosive devices.

Mohammad Younis was arrested by FBI and other agents of a related antiterrorist squad. Younis, 45 years old, was found guilty under one charge – implementation of money transfers without a proper license.

#### Case Study 3.6.7.2. Use of Hawala-like systems by terrorists

---

Under the case of money transfers implemented by terrorists from the Indian **Terrorist Organization X** through Hawala-like systems, two Hawala operators and two recipients of the money transfers amongst terrorists were arrested. Approximately INR 2 million were seized from them in the process (equivalent to USD 32,000).

They reported that the above money was provided for transfers by the leaders of the organization based in the **Country Y** and heading for the **Country Z** where a “legal employee” of the terrorist organization was located.

The system used the following principle for its operations. The terrorist leader in the **Country Y** collected money from terrorists on his territory and sent it to another agent of the organization located in the **Country Z**. The latter, in his own turn, approached the operators of an informal payment system freely operating in the above country (it is obvious that Hawala-like systems are not banned in the **Country Z**). An operator in the **Country Z** gave the agent a certain banknote number and phone of a individual who would transfer money to India. Afterwards, the agent notified the terrorist leader in the **Country Y** thereof. The latter in the **Country Y** contacted the “legal employee” of a related terrorist organization in Deli and passed him the Hawala operator’s number as well as the acquired banknote number. Then the employee called the operator with the provided number and acquired money in a set place by

notifying the banknote number. The “legal employee” could not identify the Hawala operator since he handed money without taking his motorcycle helmet off. At the same time, the terrorist agent paid no additional fees when receiving the money.

A law enforcement authority is in the middle of a related investigation.

### **Case Study 3.6.7.3. Use of principles of informal payment systems for terrorism financing in Ukraine**

---

In order to finance terrorist groups on the temporarily occupied territory of Donetsk Oblast, the **Citizen of Ukraine G** approached a currency exchange desk in Kyiv whereat he left cash in the amount of USD 2,500 without any exchange operations or related receipts, which he referred to a representative of an ORDLO terrorist organization and provided him with an address to acquire funds.

Later, in October 2016-March 2017, the **Citizen G** implemented several transfers for terrorism financing using the above scheme.

The total amount of funds transferred for terrorism financing constituted **USD 10,000**.

In accordance with a related verdict of the court, the **Citizen** was convicted for committing a crime under Part 1 Article 258<sup>5</sup> of the Criminal Code of Ukraine considering the penalty of imprisonment for the term up to five years and a ban on entrepreneurship activities for the term of up to two years.

A law enforcement authority is in the middle of a related investigation.

**SECTION IV**  
**TOOLS AND METHODS**  
**TO FINANCE TERRORISM**  
**IN UKRAINE**

---



TRIOLOGICAL STUDIES 2017



Due to its geopolitical location, territory, climate, agricultural lands, industrial development, scientific capacity as well as military and industrial complex, Ukraine is under constant political, economical and informational pressure made by specific world countries, and especially – the neighbouring states.

Since the beginning of the Antiterrorist Operation in the ORDLO territory, the issue of terrorism has become of extreme relevance for Ukraine. In the current situation, the factor of external interference has become crucial without a doubt. All the internal pressure points in the society have been successfully used to escalate the conflict.

The biggest current threat for Ukraine is the incitement, support and use of separatist intentions from external sources. The above is ensured by providing required material resources, political and information support, diplomatic and economic pressure for the benefit of separatists.

Terrorists acting on the ORDLO territory use external support to supply weapons, military machinery, ammunition, material and financial resources as well as training for their FTFs at military proving grounds.

Both national and international media widely cover participation in the terrorist ranks operating on the ORDLO territory, great number of mercenaries, FTFs and private military companies that not only take part in the implementation of terrorist attacks but also raise funds for travels to these territories.

The so called “humanitarian convoys” guided to the territory of Ukraine have been a common case since 2014. The above convoys are disguised as aid for civilians on the ORDLO territory, but in fact they violate all possible international regulations since they are not checked either by Ukrainian border guards and customs officers or representative of the International Committee of the Red Cross. According to open sources, these “humanitarian convoys” are used to move not only arms, military machinery and cash for illegal ORDLO armed groups but also essential products and goods collected by various international charitable organizations and volunteer structures to the territory of Ukraine. The latter are subsequently sold through terrorist-controlled retail networks, and earned funds used for terrorist financing activities and wages for mercenaries.

A great number of organizations, including charitable and volunteer structures, are active in ORDLO facilitating terrorist, separatist, intelligence and sabotage operations in Ukraine. They also raise funds with the use of social networks and internet for the needs of illegal armed groups.

Other proceeds gained from various criminal activities, starting from illicit mining of mineral resources (first of all, coal), smuggling and illicit trade with companies located in neighbouring countries and specific dishonest Ukrainian traders and ending with robberies in the private sector, extortions and kidnapping, constitute a substantial source of revenues for terrorist groups active on the ORDLO territory.

Considering the fact that there is no full-fledged banking system in ORDLO, this territory has an organized system of money transfers similar to Hawala to move funds to Ukraine or the neighbouring country and back. The above system is also actively used for financing of specific terrorists and terrorist groups.



Separatism-related organizations operate on the territory of Ukraine masked as legal facilities, for instance, sport clubs or civic society organizations, sponsored by foreign funds of various property form, private persons, including representatives of oligarch structures, and marginal foreign political parties interested in escalating the pressure and destabilizing the situation in Ukraine. Separatist sentiments are also commonly promoted by ecclesiasts amongst their parishes.

As obvious from the information provided in this study, terrorist and separatist organizations active in Ukraine today use the same resource and financial sources as the most of illegal armed groups all over the world.

According to the typology study, the following vulnerabilities specific for Ukrainian realities and facilitating expansion of terrorism, separatism and financing thereof have been defined:

- lack of control over migration flows for both individuals and inventories from/to the ORDLO territory;
- substantial flow and rates of cash use;
- possible registration of economic agents to figureheads;
- lack of regulation over the non-profit sector;
- simple to use payment systems;
- shadow economic activities;
- drug trafficking, proliferation of arms and human trafficking;
- incitement of anti-governmental and anti-state sentiments among the general population.

The following sources of terrorism and separatism financing should be mentioned:

- proceeds from various criminal activities;
- donations from physical persons;
- charitable contributions;
- aid from international extremist organizations;
- aid from states interested in inciting instability in Ukraine;
- aid from representatives of foreign organizations supporting participants of illegal armed groups.

Counteraction to terrorism financing is impossible without detection and study into financial tools used for this matter. The information from the study allows concluding that there are the following most wanted tools for terrorism financing:

- cash;
- aid for relatives;
- charitable donations;
- financial aid;
- replenishment of card accounts;
- replenishment of electronic wallets;
- replenishment of cell phones;
- securities, specifically, bills, shares and investment certificates;
- assignment of claims.

Considering the issue of separatism and terrorism financing, it is also necessary to pay attention to the geographical risk. It is also worth focusing on the country of origin to detect states with level of terrorist activity.

The biggest share of funds for terrorism and separatism financing has been coming from Iraq, Turkey and the Russian Federation. According to the Global Terrorism Index Report published by the Institute for Economics and Peace at Sydney University (Australia)<sup>22</sup>, two of the above countries (Iraq and Turkey) are within the Top 10 of the world countries with the highest terrorism score placed on the 1<sup>st</sup> and 9<sup>th</sup> places, respectively.

RANK	COUNTRY	SCORE									
1	Iraq	10	10	Libya	7.256	19	Central African Republic	6.394	28	Burundi	5.637
2	Afghanistan	9.441	11	Egypt	7.137	20	Niger	6.316	29	Colombia	5.595
3	Nigeria	9.009	12	Philippines	7.126	21	Bangladesh	6.181	30	Palestine	5.551
4	Syria	8.621	13	Democratic Republic of the Congo	6.967	22	Kenya	6.169	31	China	5.543
5	Pakistan	8.4	14	South Sudan	6.891	23	France	5.964	32	United States	5.429
6	Yemen	7.877	15	Cameroon	6.787	24	Ethiopia	5.939	33	Russia	5.329
7	Somalia	7.654	16	Thailand	6.699	25	Mali	5.88	34	Chad	5.269
8	India	7.534	17	Ukraine	6.557	26	Saudi Arabia	5.808	35	United Kingdom	5.102
9	Turkey	7.519	18	Sudan	6.453	27	Lebanon	5.638	36	Israel	5.062

# GLOBAL TERRORISM INDEX 2017

<sup>22</sup> The Global Terrorism Index Report [Electronic resource]. Access mode: <http://visionofhumanity.org/app/uploads/2017/11/Global-Terrorism-Index-2017.pdf>

### **For reference**

*The Global Terrorism Index and related world country ranking are a comprehensive study of terrorist activity rates in the world and demonstrate the scale of the terrorist threat in terms of nations.*

*The Index was developed by an international expert group under the umbrella of the Institute for Economics and Peace at Sydney University (Australia). It has been published annually since 2012. Ukraine took the 17th place in the ranking 2017 by improving its position as of 2016, which was the 11th place (2015-11).*

*Improved Ukrainian ranking proves the decreased rates of terrorist threat and underlines the success in fighting against terrorism and financing thereof.*

*The following activities can be named the most popular methods to finance terrorism and separatism:*

- *money transfers through international electronic payment systems (KoronaPay, Yandex. Money, Money@mail.ru, QIWI, WesternUnion, MoneyGram, PayPal and Webmoney), electronic and web wallets;*
- *cash couriers ("mules");*
- *material support to terrorist groups through non-profit (charitable) organizations controlled by the above groups or related persons;*
- *international supplies with further payments on the territory of other countries;*
- *financing of terrorism implemented by non-residents and masked as legal activities;*
- *volunteer donation of personal cash by individuals to representatives of terrorist and/or separatist organizations;*
- *money transfers to personal card accounts held by members of terrorist groups;*
- *use of fictitious financial structures to acquire cash;*
- *use of third parties for fundraising;*
- *use of ATMs for cash withdrawals from bank accounts of third parties;*
- *use of debit cards;*
- *receiving loans (credits) without an intention to return those;*
- *use of mutual (clearing) payments to cover up money flows;*
- *direct transfer of property and other assets to third parties affiliated with terrorist activities;*
- *extortion of financial aid from economic agents for its further use to finance terrorist and separatist activities, including that by leaders of illegal armed groups active on the ORDLO territory;*
- *robberies, plunder, kidnapping of people for ransom;*
- *unauthorized debiting of accounts held by legal entities with further transfer of the above funds to accounts held by individuals and legal entities.*

## CONCLUSION TO THE PART II

Stepping up of terrorism and separatism in Ukraine forms a number of new tasks and objectives related to financing thereof and requires strict controlling measures over financial flows. Hence, the activity related to the detection and efficient blockade of financial support channels for terrorist and separatist organizations must be one of the key priorities of a related long-term strategy for public administrations. It is the terrorism financing which enables implementing terrorist attacks while ensuring related training for terrorists and their technical support.

Tracking of financial flows and transactions that can be related to terrorist activities as well as understanding of mechanisms to acquire, use and manage funds by terrorist organizations regardless of their sizes are important steps for detection and counteraction to terrorism and financing thereof.

As of now, Ukraine has been in the "hazard area" in terms of terrorism occurrence, and the situation in the east of the country is a direct reason for expansion of terrorism on the national level.

Moreover, activities of followers of international terrorist organizations related to movement or "masking" of original sources of financial assets for their further referral to reliable financial institutions of developed countries can be the most vulnerable part of Ukrainian defences.

The major factor which makes Ukraine attractive for terrorist organizations includes the high "shadowing" rates of the national economy, high cash circulation rates, significant level of society's corruption and position of specific financial institutions aimed at fundraising regardless of the origin of the above funds.

Hence, the use of relevant methods facilitates to mitigation of risks in terms of both international and national terrorism, specifically:

- efficient detection of financial transactions related to terrorism and separatism financing;
- conquering corruption;
- lowered cash flows;
- control over validity of information on beneficial owners submitted during the registration/ re-registration of economic agents;
- deshadowization of the national economy;
- quality improvement for pre-trial investigations into cases related to financing of terrorism/ separatism;
- use of target financial sanctions against persons affiliated with financing of terrorism.

Successful fight against financing of terrorism (both national and/or international) also requires constant interagency interaction between all the members of the national system of prevention and counteraction to money laundering, financing of terrorism, proliferation of weapons of mass destruction and international cooperation in these fields.

## LIST OF ABBREVIATIONS

AML/CFT	anti money laundering and counteraction terrorism financing
EU	European Union
FATF	Financial Action Task Force on Money Laundering
FIU	Financial intelligence unit
FT	financing of terrorism
FTFs	foreign terrorist fighters
G20	a group of Ministers of Finance and central bank directors from 19 biggest economies of the world and the European Union
GDP	gross domestic product
ISIL	the “Islamic State of Iraq and the Levant” terrorist organization
ML/FT	money laundering, proliferation of weapons of mass destruction and financing of terrorism
MONEYVAL	An Expert Committee at the Council of Europe involved in assessment of preventive actions to counter money laundering and financing of terrorism
ML	money laundering
NBU	National Bank of Ukraine
NRA	AML/CFT national risk assessment
NGO	non-government organization
NPO	non-profit organization
ORDLO	separate regions of Donetsk and Lugansk Oblasts
PEPs	politically exposed persons
RE	reporting entities
SFMS	State Financial Monitoring Service of Ukraine
USA	United States of America
UN	United Nations Organization
UNSC	United Nations Security Council
VAT	value-added tax
WMD	weapons of mass destruction



State Financial Monitoring Service of Ukraine  
State Institution of Post-Graduate Education "Academy of Financial Monitoring"

**Typological Studies of  
the State Financial Monitoring Service of Ukraine  
2017**

Publication and translation into English was made with the assistance of the European Union  
Anti-Corruption Initiative (EUACI)

KYIV 2018



