



**MONEYVAL**

# RESEARCH REPORT

**The postponement of financial transactions and  
the monitoring of bank accounts**

*April 2013*

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE



[www.coe.int/moneyval](http://www.coe.int/moneyval)

## **The postponement of financial transactions and the monitoring of bank accounts<sup>1</sup>**

---

<sup>1</sup> Ref. MONEYVAL(2013)8, dated 11 April 2013, adopted by MONEYVAL at its 41<sup>st</sup> plenary meeting (8-12 April 2013)

## Table of Contents

<b>1. Introduction .....</b>	<b>5</b>
<b>1.1. Background information .....</b>	<b>5</b>
<b>1.2. International standards .....</b>	<b>5</b>
<b>1.3. Literature review .....</b>	<b>6</b>
<b>1.4. Objective of the study .....</b>	<b>7</b>
<b>2. Methodology .....</b>	<b>9</b>
<b>3. Postponement of transactions in MONEYVAL states .....</b>	<b>10</b>
<b>3.1. Postponement of transaction by FIUs .....</b>	<b>10</b>
<b>3.2. Postponement of transaction – Law Enforcement .....</b>	<b>21</b>
<b>3.3. Postponement of transaction – Private sector approach .....</b>	<b>22</b>
<b>3.4. Cooperation between LEAs .....</b>	<b>28</b>
3.4.1. National cooperation .....	28
3.4.2. International cooperation .....	32
<b>3.5. Conclusions .....</b>	<b>34</b>
3.5.1. Problems .....	35
3.5.2. Red flags and indicators for postponement .....	36
<b>4. Monitoring of bank accounts .....</b>	<b>37</b>
<b>4.1. Monitoring of bank accounts by FIUs .....</b>	<b>37</b>
<b>4.2. Monitoring of bank accounts by LEA .....</b>	<b>39</b>
<b>4.3. Monitoring of bank accounts – the private sector’s view .....</b>	<b>41</b>
<b>4.4. Cooperation between LEAs .....</b>	<b>43</b>
<b>4.5. Conclusions .....</b>	<b>44</b>
4.5.1. Problems .....	45
4.5.2. Recommendations .....	45
<b>5. Annex – cases .....</b>	<b>46</b>
<b>Case 1 – Bulgaria .....</b>	<b>46</b>
<b>Case 2 – Cyprus .....</b>	<b>46</b>
<b>Case 3 – Cyprus .....</b>	<b>47</b>
<b>Case 4 – Croatia .....</b>	<b>47</b>
<b>Case 5 – Croatia .....</b>	<b>48</b>
<b>Case 6 – Latvia .....</b>	<b>48</b>
<b>Case 7 – Lithuania .....</b>	<b>50</b>
<b>Case 8 – Montenegro .....</b>	<b>51</b>
<b>Case 9 – Romania .....</b>	<b>51</b>
<b>Case 10 – Serbia .....</b>	<b>52</b>
<b>Case 11 – Ukraine .....</b>	<b>53</b>

© Council of Europe. All rights reserved. Reproduction is authorized, provided the source is acknowledged, save where otherwise stated. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-Rom, Internet, etc) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the Council of Europe, Directorate General I – Human Rights and Rule of Law, Council of Europe (F-67075 Strasbourg, at [moneyval@coe.int](mailto:moneyval@coe.int))

## Abbreviations and Acronyms

AML/CFT	Anti-Money Laundering/ Combatting the Financing of Terrorism
AMLO	Anti-Money Laundering Office (Croatia FIU)
APMLFT	Act on the Prevention of Money Laundering and Terrorist Financing (Slovenia AML/CFT Law, 2007)
CDD	Customer Due Diligence
CETS	Council of Europe Treaty System
CTR	Currency Transaction Report
DNFPB	Designated Non-Financial Professions and Businesses
ETS	European Treaty System
EU	European Union
FATF	Financial Action Task Force
FIAU	Financial Intelligence Analysis Unit (Maltese FIU)
FIU	Financial Intelligence Unit
FSA	Financial Sector Supervision Authority
IMF	International Monetary Fund
JIT	Joint Investigation Team
LEA	Law Enforcement Agencies
ML/TF	Money Laundering/Terrorist Financing
MOKAS	Unit for Combatting Money Laundering (Cypriot FIU)
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures
MVT	Money or Value Transfer
OMLP	Office for Money Laundering Prevention (Slovene FIU)
PoCA	Proceeds of Crime Act (UK Law, 2002)
RE	Reporting Entity
SANS	State Agency for National Security (Bulgarian LEA)
SAR	Suspicious Activity Report
SICCFIN	Service d'Information et de Contrôle sur les Circuits Financiers (Monaco FIU)
SOCA	Serious Organised Crime Agency (UKFIU)
ST	Suspicious Transaction
STR	Suspicious Transaction Report
UNSCR	United Nations Security Council Resolution
WB	World Bank

## 1. INTRODUCTION

### 1.1. Background information

1. This report was produced by a team of experts coordinated by Mr. Raul Vahtra (Project Leader): Ms. Kerly Espenberg (Estonia), Mr. Francis Desterbeck (Belgium), Mr. Nedko Krumov (Bulgaria) and Mr. Wojciej Paczowski (Poland), assisted by Ms. Irina Talianu (MONEYVAL Secretariat). The report also benefits from the input received from the UK FIU and from the private sector through the Swedish Bankers' Association, represented by Mr. Daniel Spritzell and Ms. Alexandra Aurusell.
2. The project commenced with an experts meeting organised in November 2011 in Tel Aviv, Israel, where all MONEYVAL delegates presented postponement of transactions and monitoring of bank accounts typologies identified in their jurisdictions. On the same occasion, the questionnaires to be completed by participating states were broadly discussed.
3. Three separate questionnaires on postponement of transactions and monitoring of bank accounts were sent to MONEYVAL delegations: one covering the perspective of the FIUs; the second dedicated to law enforcement agencies involved in pursuing/prosecuting money laundering and financing of terrorism cases; and the third seeking input from private sector representatives operating within the respective jurisdictions (banks).
4. There were 23 replies to the questionnaires and the results of the survey were used, along with information from other sources, to identify and analyse the best practices available for public authorities namely the Financial Intelligence Unit (FIU), law enforcement agencies (LEA) and the private sector, to use postponement of transactions and monitoring of bank accounts powers in a more effective manner.
5. In October 2012, a core group of experts met in Warsaw, Poland, to discuss the draft report and the conclusions drawn from the questionnaires. The three perspectives on postponement and monitoring processes (FIU, law enforcement and private sector) were discussed and an exchange of views between experts was directed towards improving and finalising the draft report.

### 1.2. International standards

6. The Council of Europe was well ahead of its time in 1980 when it adopted the first international instrument against money laundering (Recommendation No. R(80)10 on measures against the transfer and safekeeping of funds of criminal origin). In 1990, the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (ETS 141) was approved by the Committee of Ministers and opened for signature in November of that year. It entered into force in September 1993.
7. To counter the newly identified money laundering/financing of terrorism (ML/FT) threats, in 2005, the Council of Europe adopted the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS 198), also known as the Warsaw Convention.
8. The Warsaw Convention provides in an international convention standards for the postponement of transactions. Article 14 requires Parties to take measures to permit urgent action to be taken by FIUs or, if appropriate, other competent authorities or bodies, in order to postpone a domestic suspicious transaction. The duration of such measures shall be determined by national law. Parties are free to permit those responsible for making the suspicious transaction report to carry out the transaction in urgent cases before the suspicious transaction report is transmitted<sup>2</sup>.

---

<sup>2</sup> Each Party shall adopt such legislative and other measures as may be necessary to permit urgent action to be taken by the FIU or, as appropriate, by any other competent authorities or body, when there is a suspicion that a transaction is related to money laundering, to suspend or withhold consent to a transaction going ahead in order to analyse the transaction and confirm the suspicion. Each party may restrict such a measure to cases where a suspicious transaction report has been submitted. The maximum duration of any suspension or withholding of consent to a transaction shall be subject to any relevant provisions in national law.

9. The Convention also requires Parties to adopt such legislative or other measures to permit urgent action to be initiated by a FIU, at the request of a foreign FIU, to suspend or withhold consent to a transaction going ahead for such periods and depending on the same conditions that apply in its domestic law with respect to the postponement of transactions.
10. At the EU level, Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing also contains provisions on the suspension of the suspicious transactions. Article 24 stipulates that Member States shall require the institutions and persons covered by the Directive to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action<sup>3</sup>.
11. The monitoring of bank accounts is not formally regulated in the AML/CFT international standards but relevant FATF Recommendations require jurisdictions to establish mechanisms to rapidly identify, trace and freeze criminal property in order to develop an effective confiscation regime. The monitoring of bank accounts is considered to be such a mechanism that would permit competent governmental agencies to better determine the licit or illicit origin of transferred funds and to better substantiate ML cases. This relatively new procedure was designed to allow FIUs and LEAs to analyse movements in bank accounts of certain suspects before a criminal case is opened.

### 1.3. Literature review

12. The 2009 Egmont Biennial Census indicates that a majority of the FIUs legally have the power to postpone operations, but the extent of the FIUs' use of this administrative provisional measure for funds that are likely to be proceeds of crime is still broadly unclear.
13. The FIU power to postpone suspicious transactions was subject to a survey conducted jointly by the World Bank and the Egmont Group adopted in 2012.
14. According to World Bank and Egmont Group data, the FIUs in at least 79 jurisdictions are authorised to postpone suspicious transactions related to money laundering, associated predicate offences, terrorist financing and/or other criminal offences<sup>4</sup>.
15. The above-mentioned 2012 report shows the existence of a wide range of practices and arrangements, and some gaps or omissions, with respect to a number of important aspects of the FIU power to postpone suspicious transactions. The study also indicates that only a relatively small proportion of FIUs with the power to postpone suspicious transactions regularly use this power; while a substantial number have not used the power at all during the 3 year period covered by the study, or have done so very infrequently.
16. In addition, the paper sets out a number of recommendations to help FIU practitioners and policy makers to establish or strengthen effective legal and operational mechanisms for the postponement of suspicious transactions, while taking into account international FIU standards and the rule of law, in order to ensure that the fundamental rights of all those concerned are effectively protected. The recommendations highlight issues and associated risks identified during the study and are meant, *inter alia*, to facilitate the development of training and technical assistance initiatives with respect to the use of the FIU power to postpone suspicious transactions.
17. Finally, the report includes a number of sanitised cases provided by FIUs and, where possible, examples of FIUs' legal and practical arrangements related to several recommendations. In addition, a template for a postponement order/notice is attached to this paper that the FIUs may wish to use as guidance when drafting their own templates.
18. Other authorities' power to postpone transactions was not subject of the survey.

---

<sup>3</sup> Member States shall require the institutions and persons covered by this Directive to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with Article 22(1)(a). In conformity with the legislation of the Member States, instructions may be given not to carry out the transaction.

<sup>4</sup> This number is based on data provided in response to the Egmont 2010 Biennial Census and the Bank – Egmont 2011 survey.

19. With regard to the monitoring of bank accounts issues, there was very limited (if any) documented literature available to the project team.

#### 1.4. Objective of the study

20. The willingness of the REs to refrain from executing a transaction and to file an STR to the FIU is a key element in the overall effectiveness of the entire AML/CFT system.
21. However, a delay in performing an operation can be a problematic issue for the REs that could jeopardise their relationship with some clients. The non-execution of a transaction without the ability to explain to the customer the underlying reason, along with the implications of such behaviour, could make financial institutions reluctant to become involved in a postponement.
22. Another aspect related to administrative provisional measures is the power that might be granted to the FIU or a law enforcement authority to monitor bank accounts. This issue is of utmost importance in the general framework on combating ML/TF and has not been sufficiently researched up to now.
23. The mutual evaluation procedures of the FATF and the similar work undertaken by the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) have provided valuable insights into the problems which have arisen both in the domestic implementation of anti-money laundering measures, and in international cooperation.
24. Much progress has been made in recent years with regard to the creation of systems for the prevention and control of money laundering and the financing of terrorism, and since the mid-1990s, in establishing financial investigations aimed at confiscating proceeds from crime as part of criminal investigations.
25. The postponement of an operation is a powerful instrument in the hands of the FIUs as the entire suspicious reporting system is more effective when disclosures are made in a timely manner. The general principle of a priori reporting (i.e. before executing the financial operation) which enables the FIUs or, if appropriate, other competent authorities or bodies, to take immediate action if necessary, should be used more frequently, both by REs and competent authorities.
26. The majority of the FIUs have the legal power to postpone operations, but the inclination of the FIUs to use this administrative provisional measure for funds that are likely to be proceeds of crime is still questioned.
27. On the other hand, it was determined that not only the FIUs but other LEAs might have the power to suspend or to postpone transactions as a preventive measure. An explanation of the manner in which those LEAs use this administrative power was one of the objectives of this report.
28. Another area for investigation and a key element in the overall efficiency of the system is the degree of willingness of REs to refrain from executing a transaction and to file an STR to the FIU. Even when the legal framework has a full set of provisions enabling the REs not to execute a transaction, their practical application might generate various difficulties for the private sector which might lead to a reluctance to use them. Identifying the obstacles the private sector faces in reporting non-executed transactions and finding ways to overcome them should increase the financial institutions' use of the system and as a direct consequence, enhance its effectiveness.
29. The monitoring of bank accounts has proved to be an effective tool in tracing criminal assets. Better knowledge of methods and practices successfully used by various LEAs in MONEYVAL countries and experience exchanges between relevant public and private sector stakeholders can only facilitate more effective financial investigations and the identification, seizure and confiscation of proceeds of crime.
30. The objectives of this study are as follows:
  - Determine how often financial institutions and DNFBPs file unexecuted STRs requiring the use of postponement powers from the FIU. Are there significant differences between jurisdictions in this respect?
  - Determine how often FIUs postpone operations based on the above mentioned STRs. Is the ratio between granting/refusing the postponement relatively constant between jurisdictions?

- Identify the time-frame which FIUs have at their disposal to decide upon the postponement of a transaction. What are the best practices for effective use of this interval?
- Identify the best sources of information used by FIUs in their financial analysis in order to decide upon postponement.
- Estimate the overall value of postponed transactions.
- Identify if there is a linkage between the postponement and final outcome for LEAs and prosecution in cases following the postponement decided by the FIU.
- Determine which is the national authority empowered to order the monitoring of bank accounts.
- Determine the usual procedure in case of monitoring.
- Estimate the outcome of monitoring process in different jurisdictions.
- Determine the linkages between account monitoring and successful prosecution and confiscation in major proceeds-generating cases.
- Identify best practices of the financial institutions on filing unexecuted STRs requiring the use of postponement powers from the FIU or other authorities.
- Identify best practices of the authorities in using the postponement and the monitoring order powers.
- Identify available sources of information to be used by the authorities in their financial analysis in order to decide upon postponement or monitoring.
- Describe the overall value of postponed transactions and monitoring of bank accounts for further criminal investigations, seizures and confiscations.
- Identify the vulnerabilities and gaps in the postponement and monitoring systems.
- Identify any area for further analysis and typologies research.

## 2. METHODOLOGY

31. The initial meeting of the typologies project was held in Tel Aviv, Israel on 31 October-2 November 2011. During the meeting, the countries' delegations introduced their postponement and bank account monitoring systems. The draft questionnaires designed by the project leader were also discussed.
32. Three questionnaires were created: 1) for FIUs; 2) for law enforcement agencies that have the right to postpone suspicious transactions and/or monitor bank accounts; 3) for REs that have the right to postpone suspicious transactions and/or monitor bank accounts
33. In total, 23<sup>5</sup> responses were received. The following countries provided answers to the questionnaire: Azerbaijan, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Hungary, Latvia, Lithuania, Malta, Republic of Moldova, Monaco, Montenegro, Romania, Russian Federation, San Marino, Serbia, Slovak Republic, Slovenia, and Ukraine. Austria, Sweden and the UK also participated in the survey.

---

<sup>5</sup> Belgium, Cyprus, Montenegro, Poland provided input in Tel Aviv meeting

### 3. POSTPONEMENT OF TRANSACTIONS IN MONEYVAL STATES

#### 3.1. Postponement of transaction by FIUs

34. From the 23 countries that responded to the questionnaires, 21 have the right to postpone transactions. The exceptions were Georgia and the UK. The latter, however, is an exceptional case (see the box below) as a consent, not postponement, system is used.

#### **BOX 1**

##### **CONSENT SYSTEM IN THE UK**

In the UK, the postponement is a two-step process: the initial postponement decision is made by Serious Organised Crime Agency (SOCA), and the actual physical postponement or restraining of the funds to prevent dissipation is made by a financial investigator from the relevant LEA, including SOCA officers with operational powers, and Customs officers. The UK's FIU does not restrain the funds itself - this has to be a LEA, Customs or SOCA officer with particular powers. Through SOCA, the FIU is responsible for granting or refusing consent to carry out a prohibited act (i.e. money laundering or terrorist financing) and issuing a letter to reporting entities (REs). In practice, in about 40% of cases SOCA seeks the advice and considers the recommendation of relevant law enforcement agency (including SOCA) and Customs before issuing a decision.

A RE has to ask the UK's FIU for consent to carry out a potentially prohibited act (i.e. a money laundering offence) under the Proceeds of Crime Act 2002 (PoCA), or a Terrorist Financing Offence under the Terrorism Act 2000. The consent of the UK FIU through SOCA provides the RE with a defence against committing a money laundering or terrorist financing offence if it was unwitting; but does not protect them from knowingly committing these offences for which they can be imprisoned.

To refuse consent, a money laundering or terrorist financing investigation has to have already commenced, or commenced as a result of the request, and there should be an expectation that, in money laundering cases, the LEA or Customs officer who has recommended refusal will obtain a Restraint Order or civil freezing order within 31 calendar days from the day of refusal. These are judicial orders which only a financial investigator or civil recovery lawyer can obtain, as the FIU has no proactive powers to restrain or freeze the actual funds.

However, granting consent does not oblige REs to proceed with the transaction; nor does it imply SOCA's approval, provide criminal defence or override other regulatory requirements. Consent may also be granted for tactical reasons.

35. In all countries that participated in the survey, the FIU's power to postpone a suspicious transaction is regulated in AML/CFT laws, it is understood as a measure allowing the taking of urgent action related to the suspicious transactions and applies to all obliged entities. In practice the postponement is applied mostly in cases of banks' and financial institutions' transactions. As a rule, the power to postpone a suspicious transaction is related to terrorist financing and with the exception of Russian Federation, also to money laundering. However, in several countries this right also applies to all predicate offences of money laundering or terrorist financing, UN sanctions, EU sanctions or even to any criminal offence (see Table 1). In Monaco the FIU's power to postpone transactions also applies to suspicion of corruption cases.

**Table 1 - Offences to which the FIU's power to postpone transactions apply**

	<b>ML *</b>	<b>TF *</b>	<b>ML predicate offences*</b>	<b>UNSC R</b>	<b>EU sanctions</b>	<b>Any criminal offence*</b>
<b>Azerbaijan</b>	X	X	X	X		X
<b>Austria</b>	X	X	X	***	***	X
<b>Bulgaria</b>	X	X	X	X	X	
<b>Czech Republic</b>	X	X	X	X	X	X
<b>Croatia</b>	X	X				
<b>Cyprus</b>	X	X				
<b>Estonia</b>	X	X	X	X	X	
<b>Hungary</b>	X	X	X			
<b>Latvia</b>	X	X	X			X
<b>Malta</b>	X	X	X			X
<b>Republic of Moldova</b>	X	X	X			
<b>Monaco</b>	X	X				
<b>Montenegro</b>	X	X				
<b>Poland</b>	X	X				
<b>Romania</b>	X	X				
<b>Russia</b>		X				
<b>San Marino</b>	X	X	X			
<b>Serbia</b>	X	X				
<b>Slovak Republic</b>	X	X	X			X
<b>Slovenia</b>	X	X				
<b>UK</b>	X	X	X	**	**	X
<b>Ukraine</b>	X	X		X		

**Note**

\* The Term "Any criminal offence" includes money laundering and its predicate offences and terrorist financing.

\*\* In the UK, offences related to UN or EU sanctions are prohibited, unless under licence, but are dealt with by Her Majesty's Treasury Asset Freezing Unit and not captured under PoCA or the Terrorism Act consent provisions;

\*\*\* In Austria the Austrian National Bank is the competent national authority as regards freezing of funds according to UNSCRs and EU Sanctions.

36. The practice as to which funds the FIU's power to postpone transactions can be applied varies. In general, countries can be divided into two groups:

1. Countries where the FIU's power to postpone a suspicious transaction is limited to only those funds identified in the suspicious transactions: Azerbaijan, Austria, Bulgaria, Croatia, Estonia, Hungary, Malta, Romania, Russia, San Marino, Slovak Republic and the UK;
2. Countries where the FIU's power to postpone a suspicious transaction is not limited to only those funds identified in the suspicious transactions: Czech Republic, Latvia, Monaco, Poland, Serbia, Slovenia and Ukraine, where the FIU's right to postpone transactions applies to all transactions suspected to be related to crime.

37. With the exception of Bulgaria, Poland, Romania, San Marino and the UK, the head of the FIU has the right to decide the FIU's postponement order. In Poland, the request for postponement may be issued by the head of the FIU or by two FIU staff persons who are the holders of his written authorisation and are acting jointly. In Romania, the decision is made by the office board. In San Marino, in addition to the director of the FIU, the deputy director and, in case of their absence, the highest official person in the FIU may issue a postponement order. In the UK a law enforcement officer, a customs officer and anyone designated by the Director General of

SOCA, acting in the capacity of a constable for the purposes set in law, have the right to issue a consent notice. This means that all UKFIU staff have been authorised, but only a small team called the Consent Desk in the UKFIU actually manage the process. With respect to the Terrorism Act, only an actual police officer can refuse the consent, although the UKFIU manages the processing of requests. In Bulgaria the postponement order is issued by the Minister of Finance, upon a proposal issued by the Chairperson of the State Agency for the National Security (in which structure the FIU is placed).

38. In practice, the postponement of transactions is seldom used in the countries that provided statistics about the postponement order (see Table 2).

**Table 2 Number of STRs/SARs/CTRs, FIU's monitoring orders and total value of assets related to postponed transactions**

	Number of STRs/SARs/CTRs received by the FIU			Number of FIU's postponement orders			Total value (EUR) of assets postponed		
	2009	2010	2011	2009	2010	2011	2009	2010	2011
<b>Azerbaijan</b>	584	52,530	236,961	0	0	2	0	0	425,000
<b>Croatia</b>	414	406	334	3	2	4	264,395	365,813	1,100,000
<b>Czech Republic</b>	2,224	1,887	1,970	57	140	96	7,600,000	11,500,000	32,300,000
<b>Cyprus</b>	429	512	526	17	19	20	NA	NA	NA
<b>Estonia</b>	16,999	13,655	13,536	132	201	142	32,100,000	25,900,000	39,800,000
<b>Hungary</b>	5,683	7,177	6,178	20	48	27	NA	NA	NA
<b>Latvia</b>	28,439	26,003	18,997	70	48	109	7,400,000	1,970,000	5,000,000
<b>Malta</b>	63	73	107	3	0	0	393,844	NA	NA
<b>Montenegro</b>	184	110	82	6	5	3	1,200,000	236	€99,000; \$1,295
<b>Poland</b>	13,230	17,835	27,412	103	112	316	9,000,000 PLN	59,800,000 PLN	96,100,000 PLN
<b>San Marino</b>	244	296	261	0	0	1	0	0	100,000
<b>Serbia</b>	284,201	242,751	265,009	37	33	78	NA	NA	NA
<b>Slovak Republic</b>	2,686	2,470	2,982	69	68	79	11,500,000	2,500,000	2,500,000
<b>Slovenia</b>	199	233	327	1	0	1	8,000	0	328,000
<b>Ukraine</b>				0	22	91	NA	NA	NA
<b>UK*</b>	228,834	240,582	247,601	1808 refused (from 13,618 requests)	1709 refused (from 14,334 requests)	2,197 refused (from 13,662 requests)	18,650,000	28,700,000	28,400,000

\*UK statistics run from October – September each year in line with the UKFIU Annual Report timetable.

39. Few countries have written specific postponement instructions or guidelines.

## BOX 2

### UKRAINE

The FIU uses Order No 172 On the Procedure of Taking Decision by the State Committee for Financial Monitoring of Ukraine on Suspension of Financial Transactions.

### UK

When deciding whether to issue a consent order, the following factors are considered:

- The opportunity to recover proceeds of crime (in essence, refusal of consent (i.e. postponement) should only happen if there is a realistic prospect of restraint of the funds within the timescale allowed in PoCA (31 calendar days) ;
- The impact on the RE
- The impact on third parties to the transaction
- the Consent Desk criteria/policy for granting consent in-house Home Office Guidance - the UK Home Office Circular 29/2008 on consent.

40. In most countries, the decision to postpone a transaction is based on certain indicators, even if they are not included in a formal document: the transaction is assessed as highly unusual or suspicious; checks in various databases or other sources indicate that the person(s) involved in transactions may be/are related to criminals; there is a danger that the execution of the transaction may hamper or substantially impede the seizure of proceeds of criminal activity or funds intended to finance terrorism.

41. Only in a few countries is postponement not considered as an administrative act (see Table 3). However, there is more variation among those countries where it is considered to be an administrative act as to whether the postponement order can be challenged in the court. In most countries, there are provisions in place allowing for redress in cases where the FIU's postponement order does not lead to prosecution, but results in identifiable losses to the beneficiary of the transaction or to the owner of the account. Often these provisions are set in state liability acts. In the majority of countries, the FIU staff involved in the postponement decision is shielded from civic liability for any losses suffered by the subject(s) of the postponement order.

**Table 3 Postponement order as an administrative act, redressing provisions and FIU staff liability**

	The postponement decision is considered to be an administrative act	Can the act be challenged in the court?	Redressing provisions	FIU staff shielded from civic liability
<b>Azerbaijan</b>	X			
<b>Austria</b>	X	NA***	X	X
<b>Bulgaria</b>	X	X	X	X
<b>Czech Republic</b>	X		X	
<b>Croatia</b>			X	X
<b>Cyprus</b>	X			
<b>Estonia</b>	X	X	X	X
<b>Hungary</b>	X			X
<b>Latvia</b>			X	X
<b>Malta</b>	X	X		X
<b>Republic of Moldova</b>	X	X	X	X

<b>Monaco</b>	X	NA		X
<b>Montenegro</b>	X		X	X
<b>Poland</b>	X		X	X
<b>Romania</b>	X	X	X	
<b>Russia</b>	X	X	X	X
<b>San Marino</b>	X*	X		X
<b>Serbia</b>	X	NA	X	X
<b>Slovak Republic</b>			X	
<b>Slovenia</b>	X	NA	X	X
<b>UK</b>	X	X**	X	X
<b>Ukraine</b>				X

**Note**

- \* In San Marino, the postponement order is an administrative act and every administrative act can be challenged under the San Marino law. In practice, this has never happened.
- \*\* In the UK, all consent decisions can be challenged in court, however the RE is not allowed to inform the subject that consent has been sought and/or refused; so it would only be an issue if the subject sued the RE for failing to carry out their instructions that consent would be challenged and SOCA would need to provide the RE with help as to how to respond.
- \*\*\* Currently the customer or another party concerned is entitled to lodge a complaint with the Independent Administrative Tribunal regarding violations of his/her rights. However, a new legislative proposal envisages that the act can be challenged before the federal administrative court. This amendment will enter into force by 1 January 2014.

42. Technical instructions on how to deal with the postponement process do exist in various jurisdictions but there is no guidance on how the responsible authority should satisfy itself in order to decide upon issuing a postponement order.
43. In almost all the countries that participated in the survey there is no practice of FIU's postponement orders being challenged in court. Neither have losses suffered by the subject(s) of the postponement order been compensated as a state liability. The UK has had several consent decisions judicially reviewed (challenged in court), but there has been no state liability compensation ordered. The challenges have resulted in changes to the interpretation of the Proceeds of Crime Act 2002 or consent procedures.
44. In a majority of countries there is no mandatory time period set in law for the FIU to issue a postponement order after receiving the STR or a request from the other authorities (see

45. Table 4). However, the FIUs usually react as quickly as possible in order to decrease the risk of negative consequences to the RE or the individuals involved in the transaction. In the UK, the FIU has 7 working days to decide whether to grant or refuse consent. In Poland, the FIU has to react within 24 hours of the immediate confirmation of receipt of the STR; otherwise the transaction will fall outside its powers (see Box 3 below). The rapid reaction of the FIU is needed in order to detect possible crimes. In case of urgent circumstances, several FIUs – Azerbaijan, Czech Republic, Croatia, Estonia, Serbia, Slovenia, and the UK – have the right to issue an oral postponement order. In these cases, the written order must usually follow within 24 hours. In other countries, even if not prescribed by the Law, an oral postponement order may be issued based on practice and good cooperation with the private sector.
46. The following table (Table 4) sets out the permissible delay allowed for the FIU to decide to issue a postponement order.

**Table 4 - The delay for the FIU to decide to issue a postponement order**

	up to 1 day/24 hours	2 business days/48 hours	Other limit	No limit
<b>Azerbaijan</b>		X		
<b>Austria</b>	X			
<b>Bulgaria</b>				X
<b>Czech Republic</b>	X			
<b>Croatia</b>				X
<b>Cyprus</b>				X
<b>Estonia</b>	X			
<b>Hungary</b>				X
<b>Latvia</b>				X
<b>Malta</b>			X*	
<b>Republic of Moldova</b>	X			
<b>Monaco</b>				X
<b>Montenegro</b>				X
<b>Poland</b>	X			
<b>Romania</b>		X		
<b>Russia</b>		X		
<b>San Marino</b>				X
<b>Serbia</b>				X
<b>Slovak Republic</b>				X
<b>Slovenia</b>				X
<b>UK</b>			X**	
<b>Ukraine</b>	X***			X

**Note**

- \* FIAU is required to oppose a transaction for a period of time within which the RE would be required by the customer to carry out the transaction. In fact, the law specifically requires the RE to inform the FIAU of the period of time within which the transaction is to be executed;
- \*\* 7 working days, followed by 31 calendar days for a judicial order to restrain the funds.
- \*\*\* Detected financial transactions related to terrorist financing: without delay (in the day suspicions arise). Further suspension of financial transaction (if the transaction was suspended by the RE): no later than the business day following that of submission of notification on suspension by the RE.

47. The duration of the postponement order is a very important aspect of the postponement system. The duration must be long enough to allow the FIU to perform a preliminary analysis and at the same time as short as possible to avoid unnecessarily prohibiting legitimate transactions. The maximum duration for a postponement order is the shortest in Malta (24 hours), the other extreme being Estonia, where the FIU can postpone transactions for 90 days and, with the permission of the administrative court, this can be prolonged to a year (see Box 3). Other long durations include Republic of Moldova and Russia (30 days), Latvia (45 days) and Austria, where the maximum postponement period is 6 months. In the majority of countries participating in the survey the maximum duration of the postponement order is 72 hours.

48. There is a relationship between the maximum duration of the postponement period and the opinion whether it is sufficient. Countries that have less than 48 hours postponement delay tend to consider it too short. The survey revealed that a good practice in setting the appropriate duration of the postponement period is to determine it based on the particular risks identified in each jurisdiction.

49. For example, in Malta, the 24-hour period was initially considered as sufficient. However, more recent studies carried out to evaluate the effectiveness of the postponement system indicated that an extension to a 3 day period would be desirable and more effective, enabling the FIU to conduct a more in-depth analysis.
50. Several delegations shared the opinion that although in general the maximum duration of the postponement is sufficient, problems can arise in cases where additional information needs to be asked from foreign FIUs, as it takes additional time to obtain a response for foreign authorities.
51. Only four countries out of 19 can prolong the postponement order. In Ukraine, the RE has the right to suspend a financial transaction for a period of up to two business days. The FIU of Ukraine can take a decision on further suspension of the transaction for up to five business days. If there is a confirmed reasonable suspicion, the FIU of Ukraine prepares and submits the relevant case referrals to law enforcement authorities. In this case, the term for financial transaction suspension shall be prolonged for seven business days on the condition that the overall term would not exceed fourteen business days.

**BOX 3****ESTONIA**

The Estonian FIU may issue an order to suspend a transaction and to impose restrictions on the disposal of an account or other property constituting the object of the transaction, professional operation or professional service or other property suspected to be related to money laundering or terrorist financing for up to 30 days as of the delivery of the order in case of ML or TF suspicion. In the event of property registered in the land register, ship register, Estonian Central Register of Securities, traffic register, construction register or another state register, the Financial Intelligence Unit may, in the event of a justified suspicion, restrict the disposal of the property for the purpose of ensuring its preservation for up to 30 days. Before expiry of the term, a transaction may be entered into or the restriction of disposal of an account or other property may be derogated only upon the written consent of the Financial Intelligence Unit.

In addition, the FIU may, on the basis of an order, restrict the use of property for up to 60 days for the purpose of ensuring its preservation if:

- 1) during verification of the source of the property in the event that there is a suspicion of money laundering, the owner or possessor of the property fails to submit evidence certifying the legality of the source of the property to the Financial Intelligence Unit within 30 days as of the suspension of the transaction or as of the imposition of restrictions on the use of the account or the other property; or
- 2) there is suspicion that the property is used for terrorist financing.

The competent authority informs the FIU immediately after.

If it is not possible to establish the actual owner of the property, the Financial Intelligence Unit may ask for permission from the administrative court to postpone the disposal of property until identification of the actual owner of the property, but for no longer than a year. The owner of the property has a right to submit an explanation to the court.

The FIU or the Prosecutor's Office may apply to an administrative court for permission to transfer property to state ownership if, within a period of one year as of establishment of the restrictions on the disposal of the property, it has not proved possible to establish the owner of the property. The court decides whether to give permission in the court session. In the event where possession of movable property or immovable property is relinquished, the property shall be sold pursuant to the procedure provided in the Acts regulating enforcement procedure and the amount received from the sale is transferred to the state budget.

**REPUBLIC OF MOLDOVA**

In the Republic of Moldova the FIU can postpone suspicious transactions for 5 days and, if there is a need for additional measures to be performed, can request the court to prolong the postponement for a period of 30 days after the expiration of this period.

**SLOVAK REPUBLIC**

The obliged entity shall be obliged to postpone an unusual transaction if there is a danger that its execution may hamper or substantially impede seizure of proceeds of criminal activity or funds intended to finance terrorism or, if so requested by the Financial Intelligence Unit in writing, until reception of notification from the Financial Intelligence Unit to carry out the transaction, under 48 hours; after expiry of this period the obliged entity shall be obliged to postpone the unusual transaction on the basis of the Financial Intelligence Unit's notification that the case has been submitted to law enforcement authorities, under 24 hours.

**UK**

After receiving a suspicious activity report asking for consent, a variety of databases is checked to identify if the subject is of interest to a LEA. If the subject is of interest to a particular LEA, consent is sent to them to make a consent recommendation. If the subject is not of interest to any LEA, but a large amount of money is being sent overseas, or the transaction meets another designated criteria, the UKFIU will forward it to the LEA located where the subject lives to make a consent recommendation. When the LEA makes a recommendation, the UKFIU tests it for proportionality and effectiveness as per the Home Office Circular 29/2008; and issues the letter granting or refusing consent. The UKFIU can overturn an LEA's decision if it does not meet this test, but this option is seldom used. If it does not meet the initial criteria to be sent to an LEA, the UKFIU can grant consent in-house. SOCA (UKFIU) is the only agency able to issue a letter of consent or refusal to the reporting sector.

52. In several countries there is an external oversight or review of the FIU's decisions to issue a postponement order. There are usually two channels:

- Supervision executed by a certain institution (mostly the office of the prosecutor); or
- Possibility to challenge the postponement order in court (see Table 3).

**Table 5 Maximum duration of the FIU's postponement order**

	Maximum length of the FIU's postponement period				Is the period sufficient	Right to prolong
	24 hours	48 hours	72 hours	other		
<b>Azerbaijan</b>			X		+	
<b>Austria</b>				X (6 months)	Depends on the case	
<b>Bulgaria</b>			X		+	
<b>Czech Republic</b>			X		+	~
<b>Croatia</b>			X		+	
<b>Cyprus</b>				X*	+	~
<b>Estonia</b>				X (30 days)	+	~ (in total 90 days)
<b>Hungary</b>	+ (Domestic transactions)**	+ (International transactions)**				
<b>Latvia</b>				X (45 days)	+	
<b>Malta</b>	X					
<b>Republic of Moldova</b>				X (5 days)	+	~ (in total 30 days)
<b>Monaco</b>			X		+	
<b>Montenegro</b>			X			
<b>Poland</b>			X		+	

<b>Romania</b>		X***			+	~
<b>Russia</b>				X (30 days)	+	
<b>San Marino</b>				X (5 days)	+	
<b>Serbia</b>			X****		+	~
<b>Slovak Republic</b>		X				~ (in total 72 hours)
<b>Slovenia</b>			X			
<b>UK</b>				X***** (31 days)	+	
<b>Ukraine</b>				X***** (14 days)	+	~

+ FIU considers the period is sufficient.

~ Right to prolong exists

\* There is no reference in the Law as to the maximum duration of the postponement period but this will not exceed a "reasonable time";

\*\* Working days;

\*\*\* If the 48-hour-period is not enough, the FIU may request to the General Prosecutor's Office, based on a reason, to extend the suspension of the operation for another period of up to 72 hours;

\*\*\*\* Plus the extension of 48 hours in case the deadline falls on a non-working day.

\*\*\*\*\* There is no deadline for restraining the funds in a refusal under the Terrorism Act - refusal is absolute.

\*\*\*\*\* On request of another FIU – according to the request.

53. External oversight over the FIU's postponement decisions is executed in following countries: Austria (only based on prior complaint), Latvia, Republic of Moldova, Russia (Prosecutor's Office), Bulgaria (Minister of Finance and chairperson of SANS), Serbia (Minister of Finance) and the UK (SOCA<sup>6</sup>). In Poland, the Supreme Chamber of Control performs ad-hoc reviews of the postponement decisions.

54. There are several procedures and measures used in order to prevent the misuse of the FIU's postponement power:

#### Multi-phase decision making process

For example, in Azerbaijan, a three-step decision-making process is used. First, the analyst makes the postponement proposal to the head of the analysts who looks through the case and decides whether to forward it to the director of the FIU. When the case is forwarded to the director, the director has to take decision on the postponement order.

#### Internal procedures

In several countries there are internal rules regulating the postponement process.

#### Informing other LEAs

For example, in Austria, Croatia and Ukraine, the FIU needs to inform the competent prosecutor's office and only the prosecutor can give the order to release the postponed transactions. In Bulgaria, there is a joint responsibility with the Minister of Finance.

#### Informing the suspected person

In several countries (for example in Austria) the suspected person has the right to complain against the order.

#### Short duration of the postponement order

The survey revealed that the tipping-off is a serious issue when it comes to the postponement of transactions. The requirement to report suspicions is not of much use if the suspected person is tipped off to the fact that s/he is under investigation. In order to preserve the integrity of an investigation, the offence of 'tipping off' occurs when information of any kind which might prejudice the investigation is disclosed to the suspect of the

<sup>6</sup> SOCA legal reviewing decisions on an ad hoc basis, and the judicial process by which all UKFIU decisions, can be subject to judicial review. There have been several judicial reviews of UKFIU consent decisions.

investigation (or anyone else) by someone who knows or suspects (or, in the case of terrorism, has a reasonable cause to suspect) that a suspicious transaction report was sent to the FIU, that an investigation into money laundering has begun or is about to begin, or that the police has been informed of suspicious activities. It also applies to cases of disclosures being made to another employee under internal reporting procedures.

55. The case studies and the discussions held with the FIU experts revealed that, during their work, at certain moments in time, specific trends are detected which are frequently encountered in the FIU's analysis having very similar features ("dynamic typologies"). A constant and swift communication to the private sector of those trends and of their features will greatly assist the private sector in detecting high risk transactions that could be subject to postponement.

#### **BOX 4**

##### **Armenia**

In Armenia, the FIU provides REs with data necessary for the identification of persons or with typologies based on which REs are obliged to suspend the business relationships or transactions matching in names (titles) or typologies.

##### **Slovak Republic**

In the Slovak Republic, information about the modus operandi is routinely circulated to the obliged entities by the FIU.

### **3.2. Postponement of transaction – Law Enforcement**

56. The survey revealed that, with two exceptions (Monaco and Azerbaijan), the LEAs cannot postpone suspicious transactions and operations. When permitted, the postponement can be made for transactions and operations related to money laundering, terrorism financing, corruption and all the predicate offences for money laundering. In Azerbaijan, suspicious transactions and operations related to any criminal offence can be postponed. All REs are covered by the power to postpone of the LEAs.
57. For LEAs, the power to postpone suspicious transactions is limited only to those funds identified in the specific transaction.
58. The power to postpone suspicious transactions/operations is provided in the AML/CFT Law and in the Criminal Code. The factors that can determine a postponement decision are mainly related to the internal analysis made by LEAs based on an STR or on a Prosecutor's request. However, no guidelines and methodological documents are available to assist the officers in making their analysis.
59. The postponement is considered differently by LEAs: in some cases as an administrative act or as a part of the criminal procedure.

#### **BOX 5**

##### **The postponement process in Monaco**

The LEAs have the power to postpone transactions at the request of the Prosecutor, of the FIU or based on their own analysis. If there is an emergency or if the case is considered serious, the FIU (SICCFIN) has the power to postpone the suspicious transaction which has been previously reported in an STR. The postponement shall be notified before the date fixed for the transaction and shall not last more than 3 days from the date of the notification. If the postponement has to be extended, a judge will need to authorise it.

If the prolongation of the postponement is necessary after the 3-day-period, the LEA must inform the Prosecutor's Office and the Court.

There are documented procedures according to which the LEAs can receive feedback on postponement orders, to ascertain whether the public prosecutor decides to freeze the assets involved in the postponed transaction, as well as on the outcome of an investigation or prosecution related to the postponed transaction(s).

60. In Azerbaijan, the postponement powers are stipulated in the Criminal Code, and the order is issued by the court on the basis of the application of an investigator and under the reference of a prosecutor within the framework of any criminal case. It is not possible to give a postponement order orally.
61. The maximum permitted duration of postponement order varies and depends on the perception of the country about the time frame needed for gathering the necessary information for further actions.
62. Where the postponement is considered a coercive procedural measure and is applied within the framework of the investigation of a criminal case, the client is informed about the procedure and there are mechanisms to protect the rights of the owners of the funds. These mechanisms are related to assets which have been postponed but where no subsequent prosecution has been conducted. Where the postponement is considered as an administrative act, the client/suspect is not informed.

**BOX 6****Azerbaijan**

The victim shall have the right to receive compensation for the damage caused by an act provided for in criminal law if the commission of this act against him is established by a court judgment or by a concluding decision of the prosecuting authority.

There are no mechanisms to protect the officials involved in the postponement decision against civil liability for losses suffered by the subject(s) of the postponement order.

63. In some cases, the postponement decision is subject to additional controls, as it is in Azerbaijan, where all decisions taken in respect of coercive measures are subject to review by the supervisory prosecutor and the court.
64. LEAs cannot postpone transactions at the request of a foreign FIU.
65. The role of LEAs in the postponement of transactions is mostly concentrated in the later stages of the process, after the suspension of the operation performed by the FIU (when the criminal procedures begin, or during the verification procedures) when LEAs provide valuable information to the FIU which might significantly influence the postponement decision.

**3.3. Postponement of transaction – Private sector approach**

66. The survey revealed that in 14 countries, reporting entities (RE) have the right granted in statutory laws to postpone transactions: Austria, Azerbaijan, Bulgaria, Czech Republic, Cyprus, Hungary, Latvia, Lithuania, Republic of Moldova, Poland, Serbia, Slovenia, Slovak Republic and Ukraine.
67. In those countries all REs (FIs and DNFBPs) have the right to postpone suspicious transactions. The survey revealed three scenarios:
- In some cases the REs have the power - explicitly provided - to postpone transactions under their own choice for the period defined by the law. This is the case in Azerbaijan, Czech Republic, Hungary, Poland, Republic of Moldova, Serbia, Slovak Republic and Ukraine. When the RE postpones a transaction it awaits the FIU's reaction. When the RE has a suspicion and does not have the powers to postpone on its own, it awaits the FIU's action.
  - In other cases, the REs refrain from executing the clients' orders. This means that during this period the RE simply do not conduct the transaction.
  - In the third scenario, the FIU's request is mandatory for the RE who has to postpone the transaction immediately. In some jurisdictions, it is admissible to execute the transaction on the customer's demand due to urgent circumstances, under the condition that the FIU is notified immediately thereafter.
68. The following table sets out the maximum permitted duration of the REs' postponement.

**Table 6 - The maximum permitted duration of the REs' postponement**

	<b>Maximum permitted period</b>
<b>Austria</b>	48 hours
<b>Azerbaijan</b>	2 business days
<b>Bulgaria</b>	allowable time provided by regulations
<b>Czech Republic</b>	24 hours
<b>Cyprus</b>	No specified limit
<b>Estonia</b>	No specified limit
<b>Hungary</b>	24 hours *
<b>Latvia</b>	24 hours
<b>Lithuania</b>	5 working days
<b>Republic of Moldova</b>	2 working days for financing of terrorism only
<b>Poland</b>	24 hours (72 hours on the FIU request)
<b>Serbia</b>	72 hours
<b>Slovak Republic</b>	48 hours
<b>Slovenia</b>	72 hours (after decision of the FIU)
<b>Ukraine</b>	2 working days

**Note**

\* For international transactions 2 working days (the period starts after the day of the suspension)

69. The postponement period is considered in different manners: some jurisdictions consider the REs' early action as the starting point for the postponement period, others the FIU's decision. The REs are not allowed to prolong the postponement. Those powers are reserved to state authorities, namely the FIUs. However, in Lithuania, it can occur when an agreement with the client allows the RE to prolong the postponement.

70. The situation is different when the requirements of the United Nations Security Council Resolutions (UNSCR) are included in the postponement system as emphasised by Table 7 below.

**Table 7 - Offences to which the reporting entities may apply their powers to postpone transactions**

	<b>M L</b>	<b>T F</b>	<b>ML predicate offences</b>	<b>UNCS R</b>	<b>EU sanctions</b>	<b>Any criminal offence</b>
<b>Austria</b>	X	X	X	X	X	
<b>Azerbaijan</b>	X	X		X		X
<b>Bulgaria</b>	X	X	X	X	X	
<b>Cyprus</b>	X	X	X			X
<b>Czech Republic</b>	X	X	X	X		X
<b>Estonia</b>	X	X	X	X	X	
<b>Hungary</b>	X	X	X			
<b>Latvia</b>	X	X				
<b>Lithuania</b>				X		X
<b>Republic of Moldova</b>		X				
<b>Poland</b>	X	X			X	
<b>Romania</b>	X	X				
<b>Russia</b>		X				
<b>Serbia</b>	X	X	X	X	X	X
<b>Slovak Republic</b>						X
<b>Slovenia</b>					X*	

<b>Sweden</b>				**	**	
<b>Ukraine</b>	X	X		X		

**Note**

\* Acting within their own capacity, the REs are entitled only to postpone in EU sanctions cases

\*\* The Swedish answer indicates UNSC and EU sanctions, but only upon a prosecutor or a judge order, not simply within the RE's or the FIU's capacity.

71. The overall assessment of the length of postponement, in a view of identifying suspicious origin of assets and suspicious of money laundering, was, in vast majority of the REs' views, positive. However, difficulties arose with respect to the manner of measuring the postponement period, which in some jurisdictions is expressed in hours and, in others, in days. The private sector expressed the view that it is better to define the time period in "days" rather than in "hours".
72. The survey revealed that there is a close link between the decision to begin the postponement procedure (regardless of the nature of the process) and the identification of the beneficial owner of the funds involved. In fact, in order to comply with the identification of the beneficial owner requirements, the REs refrain from executing transactions where there are doubts about his/hers identity. This was considered as a good practice and a valuable indicator for possible postponement.
73. The powers of the REs to postpone STs are usually stipulated in AML/CFT laws.

**BOX 7****Slovenia**

In Slovenia, the postponement can be executed only upon request from the FIU, thus the REs do not have the right to postpone based on their own suspicions. They do not need to refrain from execution of transactions, but carrying out the transactions should be supported by an STR sent to the FIU.

As regards the postponement of transactions in Austria the general rule regarding the financial sector states that credit institutions and financial institutions have to refrain from any further execution of the transaction until the matter is resolved, unless there is danger that a delay in the transaction may complicate or prevent the investigation of the case. In cases of doubt, orders involving incoming funds may be executed, while orders involving outgoing funds are not to be executed. Credit institutions and financial institutions are entitled to request that the FIU decides whether concerns exist about the immediate execution of a transaction; if the FIU fails to respond by the end of the ensuing banking day, the transaction may be executed immediately.

74. As regards the non-financial sector the general rule were that these REs have to refrain from further execution of the transaction if upon their request the FIU fails to decide whether concerns exist about the immediate execution of a transaction by the end of the ensuing working day. In that case the transaction may be executed immediately. Should the REs avail themselves of the need to extend the range of postponement, this is often done by postponing other transactions on the account, related to other activities REs host. In some jurisdiction there is a possibility of freezing not only one single transaction, but all suspicious funds and transactions of a certain client.
75. As a rule, during the postponement period, the REs are obliged to cooperate only with the FIUs and no court, prosecutor, or law enforcement agency is involved. The REs act with a view of postponements only, and do not monitor the future freezing or confiscation, or assets handling under criminal and court proceedings.
76. A particular situation is related to asset freezing in the field of the implementation of UN sanctions regimes where the process is pursued in contacts with other institutions (e.g. the Central Bank in Austria). In Ukraine, in case of suspicion of financing of terrorism, the REs are required to send the notification to the competent law enforcement authorities as well as to the FIU.
77. For the REs a swift reaction from the FIU is crucial because once the notification has been submitted, the postponement commences. In some jurisdictions, the FIU must inform the RE even when the postponement has not been approved; in others only when the postponement is granted (the silence of the authorities equals the release of the operation). The survey revealed

that REs prefer the first option because the absence of the competent authorities' (the FIU) reaction creates uncertainty about further measures to be taken on the transaction. The private sector pointed out the electronic banking transactions which require even more urgent action from the FIUs to effectively hold back the suspected criminal funds.

78. The REs sometimes have to face situations where there is no prosecution after postponement. In such cases, they are secured by the law shifting liability to state authorities but the relationship with the client might suffer.

#### **BOX 8**

##### **Slovak Republic**

In the Slovak Republic, when in doubts, there is a presumption of good faith, but the liability for eventual damage shall be borne by the State, and indemnities shall be paid by the Ministry of Interior. In the Czech Republic and Serbia only losses which are the result of intentional or gross negligence may be the RE's liability.

79. The REs do not fear the option that they may be taken to court. There is no civil redress for any person affected by a postponement against a RE or its personnel.
80. Additional procedures against the misuse of postponement powers are not deemed necessary both by the REs and by the regulatory bodies. The REs consider the postponement system as being self-regulatory as a postponed transaction might be a lost transaction and may jeopardise a relationship with a client, incurring financial losses. Hence, the need to preserve the position on the market and good relationships with clients from one side, and the legal provisions forcing the postponement of suspicious transactions on the other side, create the desired balance.
81. The REs do not have any specific internal safeguards to avoid misuse of the postponement powers. The AML/CFT legislation and internal procedures define the manner of internal control including the postponement actions.
82. The decisions on postponements are taken by the RE's management: the Director, alone or jointly with the compliance officer. There is a peculiarity noted in Bulgaria where the RE's employee responsible for postponing a transaction acts independently and his decision to postpone the transaction cannot be cancelled by the management or at a more senior level. The internal AML/CFT procedures prescribe the process and the level of decision in postponement cases.
83. In some cases, for the DNFBP, there can be an intermediary between the RE and the FIU, in which case, there is a need for the intermediary to act expeditiously.

#### **BOX 9**

##### **Lithuania**

Lawyers or lawyers' assistants immediately report a suspicion to the Lithuanian Bar Association, which in turn contacts the FIU.

##### **Poland**

In Poland the national self-managing body of notaries, attorneys, legal advisers and foreign lawyers submits the list of persons responsible for providing such information to the FIU.

84. In general, the clients are not informed about postponement by the RE. There is no requirement for the RE to advise the client when a postponement is about to run either. The lack of information to the clients is a result of a tipping-off prevention and confidentiality provisions.

**BOX 10****Serbia**

In Serbia, if the client asks about the delay of the transaction, the RE must answer, but the answer can be limited to the fact that the delay was requested by a state authority, without providing further details.

**Slovak Republic**

In the Slovak Republic, it is possible to answer to the client that circumstances fall under the AML act and secrecy requirements.

**Latvia and Russia**

In Latvia and Russia, the RE has to inform the client.

85. The survey revealed that the REs encounter difficulties in identifying the degree of “suspicion” that would require a postponement, as opposed to a “usual” STR. The REs are competent in self-reliance as regards both a detection of suspicious transactions and the postponement.
86. Interviews with various stakeholders pointed out that a significant part of STs resulting in the suspension of a transaction are generated from the MVT system and not by bank transfers. The banks are indeed the REs carrying out the entire process, but in their capacity of MVT agents.
87. Also, the survey revealed that, frequently, an element triggering the postponement report is related to countries that do not apply or insufficiently apply the FATF Recommendations, especially if this element is combined with other grounds for suspicion.
88. In detecting money laundering and terrorist financing crimes, REs are sometimes constrained by indicators provided for by the law. Often, the REs use two sets of rules in a tandem – stemming from the law and internal rules. The obligation to implement internal organisational AML/CFT rules is commonly followed by more detailed guidance like indicators and instructions for employees. In some countries, RE can simply rely on their own internal rules, as in the Czech Republic. Sometimes internal rules are completed with FIU and financial supervision blueprints and recommendations, as in Serbia and Ukraine.
89. The personal assessment of the bank employee grounded in certain factors (KYC information, risk assessment of the client, purpose and the aim of transaction, amount of the transaction, purpose and intended nature of a business relationship, type of business and business activities of a customer, related parties, turnover per customer account, etc.), remains a key element in the postponement decision.

**BOX 11****Azerbaijan and Serbia**

In Azerbaijan and Serbia, REs benefit from red flag indicators issued by the FIU.

**Hungary**

In Hungary, some lists of unusual transactions by Hungarian Financial Supervisory Authority are considered as guidance.

**Lithuania**

In Lithuania, there are general AML/CFT guidelines issued either by the FIU or by supervisory authorities. In a few countries, REs do not have such guidelines.

90. The main problem related to postponing STs which REs face in practice is the non-disclosure requirement. The RE’s employee needs to explain to the client the reasons for a delay in executing the transaction and in delivering the money/assets to their owner. Generally, the AML/CFT law does not define the way of dealing with the client whose transaction is postponed; therefore, many particular issues have to be managed on their own by RE to avoid tipping off.
91. The survey emphasised that REs are aware of the possible harm to their reputation in cases of tipping off. That question is raised during internal and external training sessions. In some

countries, a bank employee is liable for financial losses incurred by the bank on tipping off grounds.

92. RE indicated that exposure to the client's demands causes difficulties and thus calls for careful handling of the contact, with the client on one side and collateral contacts with the FIU on the other side.

#### **BOX 12**

##### **Slovenia and Sweden**

In Slovenia and Sweden, in postponement cases the REs are in close contact with the FIU which instructs them what can and cannot be told to the client in particular circumstances. In Slovenia, the FIU can give the bank an oral instruction under the AML/CFT law on how a particular situation should be dealt with.

93. The private sector indicated some actions to be taken that could diminish the difficulties they face in the postponement cases:

- Guidance and best practices issued by the authorities, particularly on postponement matters;
- Guidance on the manner in which the REs should communicate with clients during the postponement period;
- to a certain extent, REs could be allowed to advise clients on the suspension of the operation;
- shortening the period of the suspension;
- Specific training provided to the private sector by the authorities;
- Shifting the burden of communication with the clients onto the FIU.

94. However, some answers indicated that financial institutions should have the discretion to decide what to tell customers, even in postponement cases. The need for international exchanges of best practices on communication with clients was also expressed by the private sector.

95. The REs are liable for an ex-post oversight of postponement activities. Supervisory bodies have that responsibility, primarily banking supervision authorities (Poland, Serbia, Slovak Republic, Slovenia, Ukraine), or external audit services providers (Lithuania). In many countries, like the Czech Republic, Poland and Slovak Republic, postponement cases are also reviewed by FIUs.

96. The oversight of postponement activities is generally foreseen by REs as effective.

97. The overall REs' assessment of effectiveness of national postponement system was positive.

#### **BOX 13**

##### **Lithuania**

In Lithuania, RE indicated that the feedback from the FIU showed positive results.

##### **Austria**

The REs from Austria provided a negative assessment of the effectiveness of the system without pointing out any particular reason.

##### **Sweden**

The lack of reaction from FIUs was mentioned as a shortcoming. According to information provided through the Swedish Banker's Association, REs from Sweden did not avail themselves of having an efficient system and there was a belief expressed that the future system allowing postponement will be helpful.

98. Some stakeholders in the banking sector suggested limiting the obligation of postponing to transactions above a certain threshold (e.g. €15,000). For lower sums, the obligation might be

left at the discretion of the RE on a case-by-case basis. Replacing the postponement for a monitoring mechanism was also proposed.

## 3.4. Cooperation between LEAs

### 3.4.1. National cooperation

99. The cooperation between law enforcement agencies is of paramount importance in ensuring the effectiveness of the postponement system. In most countries participating in the survey, there is some kind of communication between law enforcement agencies.

100. As a rule, the FIU can postpone a transaction based on a suspicious transaction report (see Table 8). In a majority of countries, it is also possible to postpone based on the FIU's own analysis or on a request from a foreign authority. The postponement of suspicious transactions at the request of police forces or of the prosecutor's office is allowed in a limited number of countries.

**Table 8 Factors that can trigger the use of the FIU's power to postpone suspicious transactions – national level**

	STR from a RE	FIU's own analysis	Request from the police	Request from the Prosecutor's office
<b>Azerbaijan</b>	X			
<b>Austria</b>	X	X	X*	
<b>Bulgaria</b>	X			
<b>Czech Republic</b>	X	X	X	
<b>Croatia</b>	X	X		
<b>Cyprus</b>	X	X	X	X
<b>Estonia</b>	X	X	X	X
<b>Hungary</b>	X	X	X	X
<b>Latvia</b>	X	X		
<b>Malta</b>	X			
<b>Republic of Moldova</b>	X	X	X	X
<b>Monaco</b>	X	X		
<b>Montenegro</b>	X	X		
<b>Poland</b>	X	X		
<b>Romania</b>	X			X
<b>Russia</b>	X	X	X	X
<b>San Marino</b>	X	X	X	X
<b>Serbia</b>	X	X	X	X
<b>Slovak Republic</b>	X	X	X	X
<b>Slovenia</b>	X	X		
<b>UK</b>	X			
<b>Ukraine</b>	X	X		

**Note**

\*In Austria the FIU is a Police type.

101. The obligation to inform other agencies in cases where a transaction is postponed is generally an exception for FIUs. As a rule, neither the court nor a financial supervision authority is informed by the FIU in cases where a transaction is postponed. However, in some countries the FIU is required to inform the prosecutor's office. The survey revealed that there are

instances where the LEAs inform the FIU about cases where postponement should be avoided as this would jeopardise an on-going investigation.

102. Most FIUs cannot postpone transactions on behalf of other national authorities. Usually, a suspicious transaction report (or in the case of a foreign request, a rogatory letter) is needed. However, in Hungary, the FIU can postpone transactions on behalf of the police and the prosecutor's office; in San Marino, it can do so on behalf of the prosecutor's office or a court. The following table sets out the obligation to inform partner agencies.

**Table 9 Informing obligations between FIU and other law enforcement agencies**

	<b>FIU to other agency After the postponement</b>	<b>FIU to other agency Before the expiry of the postponement</b>	<b>LEA to FIU</b>
<b>Azerbaijan</b>	Prosecutor's Office Ministry of National Security**		X
<b>Austria</b>	Prosecutor's Office Client	X	X
<b>Bulgaria</b>		Prosecutor's Office	
<b>Croatia</b>	Prosecutor's Office	X	X
<b>Cyprus</b>	No obligation	No obligation	No obligation
<b>Estonia</b>	Client	X	X
<b>Hungary</b>			X
<b>Latvia</b>	Client		X
<b>Malta*</b>			
<b>Republic of Moldova</b>	Client	X	
<b>Monaco</b>		X	X
<b>Montenegro</b>	Prosecutor's Office Police Directorate	Prosecutor's Office Police Directorate	X
<b>Poland</b>	Prosecutor's office		X
<b>Romania</b>	Prosecutor's Office		X
<b>Russia</b>	Prosecutor's Office Client	X	X
<b>Serbia</b>		X	X
<b>Slovak Republic</b>		X	X
<b>Slovenia</b>	Prosecutor's Office Court		X
<b>UK***</b>		X	X
<b>Ukraine</b>	Prosecutor's Office LEA	X	X

**Note**

\* Malta's FIAU is not required to inform any other authority. However, in practice, the FIAU informs the police of any such transaction and, where it is established that a suspicion of ML/FT subsists, the attorney general is informed and can then apply to a criminal court for the issuance of an attachment order. An attachment order would effectively freeze the suspect's entire property for thirty days. There is no time-frame in the law which is applicable to these circumstances.

\*\* In relation with TF and UNSCR list.

\*\*\* FSA is the financial sector supervision authority

103. The FIU is sometimes required to consult with other institutions before the expiry of the postponement order for future freezing/confiscation. This applies in the following countries: Austria, Croatia, Estonia, Republic of Moldova, Monaco, Poland, Russia, Serbia, Slovak Republic, the UK and Ukraine. In most cases, the cooperation is relevant in deciding whether or not to freeze the assets related to postponed transactions.

104. In a majority of countries (except Bulgaria, the Czech Republic, Malta, Republic of Moldova, and San Marino) the law enforcement agency dealing with the case has a duty to report back to

the FIU on further steps to be taken. In some countries, this is done quarterly and in most countries at least once a year.

**BOX 14****UK**

The UKFIU consults with the LEA dealing with the refusal at 7, 14, 21 and 28-day intervals during the moratorium period, in order to ensure that the LEA is on track to restrain the funds within 31 days. If the UKFIU is given information that restraint will not be possible within that period, it has a duty to grant consent on the day this is identified.

There is no requirement in legislation for the law enforcement agency to inform the UKFIU of the outcome of the refusal/postponement or restraint, but general feedback to the UKFIU is a requirement of an agreement granting the LEA access to the SARs database. However, as the UKFIU follows up 4 times during the moratorium period, the information as to the outcome of the restraint is usually forthcoming from LEAs.

105. In a majority of countries that participated in the survey, the FIU does not have to inform the person whose transaction has been postponed about the postponement. Only in Austria, Estonia, Latvia, Republic of Moldova and Russia is there such an obligation. In Austria, Estonia and Republic of Moldova, the FIU or, in Latvia and Russia, the RE is required to inform the client. The client is informed as soon as possible, although there is no specific deadline set in law. In Republic of Moldova, the client is informed only if, after 5 days of postponement, the FIU requests the court to prolong the order and the decision of the court prescribes that the client must be informed, in order to respect his right of defence, as s/he may contest the decision.
106. A majority of FIUs do not have documented procedures to follow-up postponement orders to ascertain whether a designated law enforcement agency conducts further investigation of the case or if the public prosecutor decides to freeze the assets involved in the postponed transaction. Little information is gathered by the authorities on the outcome of an investigation or prosecution related to the postponed transaction(s). Only a few countries have such systems in place.

**Table 10 Number of postponement orders, investigations initiated, prosecutions and convictions based on the postponement**

	Postponement orders				Investigations				Prosecutions				Convictions			
	2008	2009	2010	2011	2008	2009	2010	2011	2008	2009	2010	2011	2008	2009	2010	2011
<b>Azerbaijan</b>	n/a	0	0	2	n/a	0	0	0	n/a	0	0	0	n/a	0	0	0
<b>Croatia</b>	4	3	2	4	0	0	0	13 (persons)	0	0	0	0	0	0	0	0
<b>Czech Republic</b>	16	57	140	96	16	57	140	96	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>Cyprus</b>	20	17	19	20	16	12	13	11	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>Estonia</b>	103	132	201	142	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>Hungary</b>	32	20	48	27	10	1	8		No answer	No answer	No answer	No answer	No answer	No answer	No answer	No answer
<b>Latvia</b>	99	70	48	109	99	70	48	109	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>Malta</b>	0	3	0	0	0	3	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>Poland</b>	320	103	112	316	197	N/A	118	26	35	N/A	27		27	18	9	4
<b>San Marino</b>	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	0
<b>Serbia</b>	60	37	33	78	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
<b>Slovak Republic</b>	N/A	69	68	79	N/A	N/A	35	51	N/A	N/A	17	28	N/A	N/A	N/A	N/A
<b>Slovenia</b>	2	1	0	1	1	1	0	1	1	1	0	1	0	0	0	0
<b>Ukraine</b>	0	0	22	91	0	0	7	5	0	0	4*	2	0	0	3*	0

**BOX 15****Austria**

In Austria, the FIU will get the copy of the freezing/confiscation order and cancellation order if the assets are unfrozen.

**Croatia**

In Croatia, it is provided by law that the FIU shall be informed when the public prosecutor freezes the assets involved in the postponement transactions. In addition, LEAs are required to inform the FIU about the outcome of an investigation initiated by a postponement operation.

**Estonia**

In Estonia, it is regulated by law that when the FIU forwards the notifications to an LEA, the LEA must immediately inform the FIU about the actions taken (freezing/unfreezing/not freezing assets).

**Poland**

In Poland, the FIU will be informed about every case of presentation of AML/CFT charges and initiation and completion of AML/CFT proceedings.

107. As Table 10 indicates, postponement is a powerful tool. In many cases, it results in investigation at later stages. For prosecutions and convictions, however, data is scarcer, as many FIUs do not trace the postponed assets or cases after the criminal procedure begins.

108. The authorities do not routinely maintain statistics on postponement issues to further analyse the effectiveness of the system.

### 3.4.2. International cooperation

109. Out of the countries participating in the survey, 15 can postpone transactions on behalf of foreign FIUs and send a request for postponement to a foreign FIU. These provisions are usually regulated in national AML/CFT laws, but several delegations also referred to the Warsaw convention. Only five countries have the right to postpone transactions based on a request by other foreign authorities. (see Table 11)

**Table 11 Factors that can trigger the use of the FIU's power to postpone suspicious transactions – international level**

	On behalf of the foreign FIU	On behalf of other foreign authorities	FIU has a right to send a request to foreign FIU
<b>Azerbaijan</b>	X		X
<b>Austria</b>	X	X	
<b>Bulgaria</b>	X	X	X
<b>Czech Republic</b>	X		X
<b>Croatia</b>	X		X
<b>Cyprus</b>	X	X	X
<b>Estonia</b>	X		X
<b>Hungary</b>	X		X
<b>Latvia</b>	X		X
<b>Republic of Moldova</b>	X	X *	X
<b>Monaco</b>			
<b>Montenegro</b>	X	X	X
<b>Romania</b>	X		X

<b>San Marino</b>	X	X	X
<b>Serbia</b>	X		X
<b>Slovak Republic</b>	X		X
<b>Slovenia</b>	X		X
<b>UK</b>	X **		
<b>Ukraine</b>	X	X	X

**Note**

\* Only in cases of common investigation.

\*\* Only in limited cases.

**BOX 15****POSTPONING THE TRANSACTIONS ON BEHALF OF A FOREIGN FIU****Bulgaria**

The Bulgarian AML Law stipulates that in cases of information received on (suspected) money laundering/terrorist financing, both from REs and through international intelligence exchange, a postponement can be carried out. The Bulgarian prosecution shall be immediately notified on the postponement and all necessary information shall be forwarded to them. The postponement lasts for three days and if no preventive measures are imposed by the prosecutor or court within this delay, the operation can be carried out.

**Croatia**

Upon receipt of a substantiated written proposal from a foreign financial intelligence unit, the Croatian FIU may, under the conditions provided for by the AML/CFT law and on the basis of effective reciprocity, issue a written order to instruct a RE to temporarily suspend a suspicious transaction execution for up to 72 hours. The FIU shall notify the State Attorney's Office of the Republic of Croatia of the issued order without any undue delay. The FIU shall take a prescribed course of action, should it deem, on the basis of reasons for suspicion indicated in the written proposal of the foreign financial intelligence unit, that:

1. the transaction is connected with money laundering or terrorist financing; and that
2. the transaction would have been temporarily suspended had the transaction been the subject matter of a domestic suspicious transaction report as provided in the AML/CFT Law.

The Croatian FIU shall not consider a postponement request from a foreign FIU if, on the basis of circumstances presented in the request, the suspicions are not substantiated. The foreign FIU shall be notified about the non-acceptance of the request and provided with the reasons for denial.

**Slovenia**

According to the AML law, the Slovenian FIU may issue a written order temporarily suspending a transaction for a maximum of 72 hours, on the basis of a reasoned and written request by an authority from a Member State or third country responsible for the prevention of money laundering and terrorist financing. The competent domestic authorities must also be informed. The Slovenian FIU may refuse the request, on the basis of facts and circumstances indicating that there are no reasonable grounds to suspect money laundering or terrorist financing. The FIU shall inform the initiator about the refusal in writing, stating the reasons for which the initiative was refused.

**UK**

If a consent request has been submitted and there is an interest from an overseas jurisdiction, the UKFIU will refuse consent on behalf of the other jurisdiction, providing they commit to an International Letter of Request (ILOR) to restrain the funds within a specified time period. The UKFIU cannot postpone transactions submitted by other jurisdictions without a UK SAR initiating the engagement. The UKFIU does not restrain the funds itself - this is done by an LEA, Customs or SOCA officer with particular powers.

110. However, there is very little practice of international cooperation in the area of postponement.
111. The survey revealed that almost all jurisdictions react swiftly to a foreign information request when a postponement operation is involved in the country generating the request. FIUs routinely communicate with each other in cases of postponements. As a rule, the requested FIU performs all the checks in the shortest time possible (less than 24 hours). The information is then sent to the FIU formulating the request. However, no formal descriptions of such processes are usually included in the cooperation documents (MoU) and the mechanism is based on the FIUs' practice.
112. Only Ukraine keeps statistics on the postponed transactions based on foreign requests. Two postponement orders were issued based on foreign requests in 2010 and 3 such requests were sent by Ukraine to foreign partners in 2011.

### 3.5. Conclusions

113. All but one delegation assessed the postponement system to be efficient in their jurisdiction. Most answers indicated that there are no significant impediments to the application of postponement obligations in their country. The survey indicates that up to 65% of them result in the freezing of the funds by Prosecution Authorities. However, in practice, the postponement of transactions is rarely used.
114. The triggering elements for postponements are: the existence of an STR (foreign requests included) and an internal analysis or prosecutor's request.
115. In general, the decision to postpone a transaction is borne by the management of the FIU or it is a collective decision within the FIU. Technical instructions on how to deal with the postponement process do exist in various jurisdictions. However, no postponement guidance as such, namely documents describing how the responsible authorities should satisfy themselves in order to decide upon issuing a postponement order, appear to have been issued.
116. The length of the postponement period has to be established through the risk assessment carried out by every country. The survey revealed that there are no "right" or "wrong" postponement periods: the duration depends on the internal factors of risks. Two groups of countries have been identified in this respect: those adopting a long period inform the clients and allow them to prove the licit origin of the funds; and those with a short period of postponement who simply "buy time" for law enforcement agencies to gather enough elements, start an investigation and use the provisional measures provided for by the criminal legislation.
117. The scope of the postponement process differs and the analysis identified two approaches: the transaction-based approach and the subject-based approach. The first approach only allows authorities to suspend assets involved in a particular transaction (usually reported on by the private sector); consequently, they cannot handle other assets owned by the individuals involved. In the second approach, the postponement can be extended to any other asset owned by the targeted individual(s).
118. With respect to the importance of postponement in the overall activity of the FIUs, the survey identified two groups: one uses postponement as a core activity (best rating: 1 postponement for 20 STRs), while others use it as a marginal practice.
119. It appears that adequate statistics are not maintained by authorities on postponement issues and therefore no overall assessment of the effectiveness of the system in the countries was carried out. This might be caused by the fact that the provisions allowing for postponements were only recently introduced. However, the survey indicated that the postponement system is considered a powerful tool for authorities in the global fight against ML, TF, financial crimes in general and criminal assets recovery. Further focus of the authorities on the results of postponement actions is needed.
120. There is no routine for the FIU to follow postponement cases after a LEA referral. This is considered a serious shortcoming as the assessment of the entire system would benefit from such information. It should be mandatory for LEAs to inform FIUs about the final outcome of the postponement cases.
121. In most countries, LEAs do not have postponement powers. Postponement is generally part of a FIU's prerogatives. However, the involvement of LEAs in the procedure is of utmost

importance in the analysis phase at FIU level and, after the issuing of a postponement order, in the initiation of the criminal procedures. When LEAs have postponement powers, they tend to assimilate it as a criminal procedure more than as an administrative procedure.

122. Only a few countries have written and formal postponement instructions or guidelines for REs. In most countries, the decision on whether to postpone a transaction is based on the general ST indicators. The private sector claims the need for specific postponement guidance to help it distinguish between ST reporting and postponement reporting.
123. There are no documented procedures for follow-up on postponement orders. Little information is gathered by the authorities on the outcome of an investigation or prosecution related to postponed transactions.
124. In a majority of countries, there is no mandatory time period set in law for the FIU to issue a postponement order after receiving an STR or a request from other authorities, but the survey revealed that usually FIUs react as quickly as possible in order to decrease the risk of negative consequences for the RE or for the individuals involved in the transaction. Oral postponement orders are possible but they must be followed by written orders shortly.
125. RE seem to need swifter assistance from FIUs in postponement cases. Oral instructions are provided in some jurisdictions but as an informal procedure. Some FIUs are reluctant to give guidance to REs on a case-by case basis, as this is not formally expressed in regulations. The inclusion of such a possibility (oral instructions to be given by the FIU to the RE in postponement cases) should be provided for by official documents.
126. A clear connection between the CDD measures and the postponement measures was identified. REs indicated that the postponement is frequently grounded on a lack of knowledge of the beneficial owner and/or the source of the money. Postponement could be an answer to difficulties encountered by the private sector in identifying the beneficial owner of the funds.
127. The private sector indicated that a significant part of STs resulting in suspension of the transactions are generated from the MVT system and not by bank transfers. In those cases, banks carry out the postponement process, but in their capacity as MVT agents.
128. The no-tipping off requirement is one of the most difficult issues a RE faces in respect to postponement cases. To address the matter, one good practice is the limitation of the number of employees that are informed about the procedure, based on the “need to know” principle. It was established that the no-tipping off requirements do not equal the postponement period in all jurisdictions.
129. Countries have taken measures to avoid tipping-off. In most countries, there are legal rules prohibiting REs (employees as well as supervisory boards, management and other persons with access to such information), FIU staff (in countries where the FIU does not inform the client about the postponement) and other third persons, from informing the person(s) related to the postponed transaction. The delegations proposed the following measures in order to avoid tipping-off:
  - Adequate regulations and sanctions
  - Short postponement periods
  - Training employees of the RE and advising on what they should tell clients when there is a delay in transaction
  - Limiting the number of RE staff who are aware of the suspicious transaction report sent to the FIU
130. There is no practice of an FIU’s postponement order challenged in court. Neither have losses suffered by the subject(s) of a postponement order been compensated as a state liability.
131. The survey indicates that postponement powers have not been abused either by the authorities, or by the private sector.

### 3.5.1. Problems

132. Frequent problems experienced by FIUs include:

- Short period for the information gathering in order to have a well-grounded postponement decision;
- Slow response of foreign FIUs in some instances;
- Slow response from LEAs in postponement cases to assist the decision process;
- No express provision in the MoU regarding the requests on postponements;
- Not enough information or identifying features in report to enable investigation or recommend a decision;
- Lack of information on the identity of the real beneficial owner; as a result the examination may not be carried out adequately and thoroughly.
- Lack of internal instructions on the manner in which the authority should “satisfy” itself that the decision to postpone the operation is opportune.

133. Frequent problems experienced by Reporting Entities include:

- Difficulties in providing explanations to the client when the transaction is delayed (the non-disclosure requirements);
- No specific guidance dedicated for postponement cases to help identify specific “postponement indicators”;
- No guidance on the degree of “suspicion” necessary to distinguish between STRs and postponement STs;
- Specific training is necessary;
- Late reaction on the FIU’s side (in a few cases);
- Lack of swift (oral) assistance on the authorities’ part in postponement cases;
- Possible damages for unjustified orders.

### 3.5.2. Red flags and indicators for postponement

134. As mentioned in the analytical part of the report, the postponement should be subject to (or part of) the national risk assessment, in order for the authorities to appropriately set the main features of the process: the postponement period, the postponement methodology and the indicators for the private sector. However, during the various meetings with the experts participating in this research, a series of indicators arose and the project team decided that it would be beneficial to list them as part of the findings of the report.

135. The red flags indicated below should be read only in conjunction with the relevant red flags and indicators for the suspicion transactions, identified by the stakeholders at the national level.

- Multiple and different suspicion elements in conjunction with large amounts of money involved in the transaction (too many uncertainties and suspicions);
- The RE has serious doubts about the beneficial owner of the funds or the origin of the funds and is incapable of verifying them;
- Information suggesting that the client is linked to a criminal activity;
- The funds originate from countries that do not apply or insufficiently apply FATF Recommendations, especially if combined with other suspicious elements;
- Transactions that match the features of the “dynamic typologies”;
- The detection of false/forged documents;
- The client was subject to previous information requests from the FIU (indication of investigations/financial analysis pending);
- Large money transfers (outgoings), suspect destinations or uncontrollable use (loss of the money trail);
- Sudden and unjustified closure of bank accounts by cash withdraws (emptying of account).

## 4. MONITORING OF BANK ACCOUNTS

### 4.1. Monitoring of bank accounts by FIUs

4. 12 FIUs participating in the survey have the right to monitor bank accounts: Bulgaria, Czech Republic, Croatia, Estonia, Georgia, Latvia, Malta, Republic of Moldova, Montenegro, Serbia, Slovenia and Ukraine. Among the countries that do not have the right to monitor bank accounts, only Azerbaijan's and San Marino's FIUs<sup>7</sup> consider that they should have such power.
5. In the Czech Republic, the FIU has the right to monitor bank accounts, but in practice it is done by the obligated persons as a part of their internal control measures. In Estonia, the monitoring of bank accounts is done only in very special cases and with the help of the bank.
6. In all countries except Republic of Moldova, the provisions enabling the FIU to monitor bank accounts are set in the AML/CTF law. In Republic of Moldova, the provisions are regulated in a law on operative investigation activities. Latvia has no real experience in monitoring bank accounts in practice. In Slovenia, The FIU's power to monitor bank accounts is used more often than the mechanism for suspending transactions.

#### BOX 16

##### Croatia

The Croatian FIU may give a RE a written order to exercise on-going monitoring of financial operations: a) of a person in relation to which there are reasons for suspicion of money laundering or terrorist financing, or b) of a person for which there are reasons for suspicion that the person has assisted or taken part in the transactions or arrangements of a person in relation to which there are reasons for suspicion of money laundering or terrorist financing.

7. The RE has a duty to inform the FIU before the execution of a transaction or entering into an arrangement, and to indicate in the report the deadline under which the transaction or the arrangement shall be completed. The process happens in real time.
8. Based on the scope of the monitoring prerogatives, countries can be divided into two groups:
  1. Those where the monitoring prerogatives apply only to money laundering and terrorist financing suspicions: Bulgaria, Croatia, Serbia and Slovenia;
  2. Those where they apply to all criminal offences: Georgia, Latvia, Malta, Republic of Moldova and Ukraine.

**Table 13 - Offences to which the FIU's power to monitor bank account apply**

	ML	TF	UNCS	Any criminal offence	Other
<b>Bulgaria</b>	X*	X			
<b>Croatia</b>	X	X			
<b>Georgia</b>	X	X		X	
<b>Latvia</b>	X	X		X	
<b>Malta</b>	X	X		X	
<b>Republic of Moldova</b>					X**
<b>Montenegro</b>	X	X			
<b>Serbia</b>	X	X			
<b>Slovenia</b>	X	X			
<b>Ukraine</b>	X	X		X	

**Note:** "Any criminal offence" includes money laundering, terrorist financing and predicate offences of money laundering and those cells are therefore not marked in the table.

\* Also predicate offences of money laundering.

\*\* Offences for which is foreseen a punishment of more than 5 years imprisonment.

<sup>7</sup> Pending new legislation. In practice the FIU has already experienced the monitoring mechanism, availing itself of the powers attributed by AML/CFT Law. In practice, the FIU invites obliged entities to monitor the accounts and to refer back as soon as something happen.

9. As a rule, the head of the FIU has the right to issue a monitoring order, which has to be issued in writing. The maximum duration of the monitoring order varies from 30 days in Republic of Moldova to 6 month in Croatia, Serbia and Slovenia. In Republic of Moldova, the Court issues the monitoring order on the proposal of the prosecutor. In this respect, the FIU should initiate the procedure by submitting a special form to the prosecutor.

**Table 14 - Maximum duration of the FIU's monitoring order**

	<b>Maximum length</b>	<b>Prolong</b>
<b>Bulgaria</b>	Depends on the case	+
<b>Croatia</b>	6 months*	+
<b>Estonia</b>	Depends on the case	
<b>Latvia</b>	2 months.	+
<b>Malta</b>	Depends on the case**	
<b>Republic of Moldova</b>	30 days	+
<b>Montenegro</b>	6 months	
<b>Serbia</b>	6 months	+
<b>Slovenia</b>	6 months	+
<b>Ukraine</b>	30 days***	+

**Note**

- \* There is no such direct provision in APMLFT. However OMLP does open cases on the base of foreign FIU requests, after which all prerogatives of OMLP can be used.
- \*\* Although in Malta this is not explicitly provided for by the law, there is nothing in the law which precludes the FIAU from issuing a monitoring order on the basis of information provided by a foreign FIU.
- \*\*\* Within the framework of tracing (monitoring) of financial transactions before the obtaining by the entity of a monitoring request (which is unrestricted). If necessary, the new monitoring order may be issued after the expiry of the previous 30-day monitoring order.

10. In all FIUs the length of the monitoring order is assessed to be sufficient. In Croatia and Slovenia, the maximum duration of the FIU monitoring order is 3 months but, with a justified reason, it can be prolonged three times, each time for an additional month, so the maximum duration of the monitoring order totals 6 months. In Latvia, a monitoring order can be issued for a month and prolonged once for an additional month but, in order to extend the duration of the monitoring order, the approval of the prosecutor's office is needed. In Serbia, the monitoring order lasts for three months with a possibility of consecutive extensions for maximum six months. In Republic of Moldova, the FIU can initiate the prolongation of the monitoring order, for up to 6 months. In Estonia, Malta and Ukraine, a new monitoring order has to be issued for the prolongation. Although in Malta there is no period of time specified in the law and a decision is taken on a case-by-case basis, monitoring orders are usually issued for a three-month period.
11. Only in two countries there is internal guidance developed to regulate the area of monitoring bank accounts by FIUs. In Latvia, it has been set under the regulation of the Cabinet of Ministers. Latvia is the only country where the FIU has to inform another authority (prosecutor's office) of the monitoring order. In other countries, there is no such obligation.
12. Generally, the FIUs are not required to follow-up with any authority before the expiry of the monitoring orders (except in cases when the suspicion is confirmed and the information sent to the police or prosecutor's office in order to start the criminal procedures and decide upon the freezing of funds). However, in some countries, monitoring orders are executed in practice in close cooperation with the police and the prosecutor's office.
13. Only in Republic of Moldova is an external oversight of the FIU's decisions on monitoring orders, performed by the prosecutor's office in the course of the planned control measures. Although there is no specific oversight for monitoring orders in Serbia, the entire work of the FIU is supervised by the Ministry of Finance.

14. Based on national experience, FIUs pointed out several factors that prevent the misuse of their power to monitor bank accounts:

- The monitoring process (and measures used to prevent its misuse) is regulated in the FIU's internal rules;
- The process is under the control of the head of the FIU;
- The external supervision over the FIU's activities encompasses monitoring orders;
- There is an appropriate and clear legal framework.

15. In order to reduce the risk of tipping off, the survey revealed that the following measures should be adopted:

- Adequate legislation (stating that the staff and management of REs as well as FIUs and other related bodies shall not be allowed to disclose information to third parties) and sanctions;
- Supervision over the issuance of monitoring orders by the head of the FIU;
- Limiting the number of staff aware of each monitoring order.

## 4.2. Monitoring of bank accounts by LEA

16. Generally, LEAs have the legal power to monitor bank accounts, with a limited number of exceptions such as Azerbaijan, Slovak Republic and Monaco.

### BOX 17

#### Slovenia

The investigating judge may upon a properly grounded proposal by a public prosecutor order a bank, savings bank or savings-credit service, to keep track of financial transactions of the suspect, the defendant and other persons reasonably presumed to have been implicated in financial transactions or deals of the suspect or the defendant, and to disclose to him the confidential information about the transactions or deals the aforesaid persons are carrying out or intend to carry out at these institutions or services. The proposal of the public prosecutor as a prerequisite of the investigative judge's order to monitor the transaction can also be issued upon a written initiative of the police. In the process of monitoring, the police will receive data from the prosecutor.

17. In most jurisdictions, the monitoring of any account can be ordered for suspicious activity related to money laundering, terrorism financing, all predicate offences for money laundering and any other criminal offence. In Lithuania, the scope is restricted to money laundering, terrorist financing and serious crimes, and other crimes indicated in the Law of Operational Activities.

### BOX 18

#### Georgia

According to the Criminal Procedure Code of Georgia, if there is a grounded supposition that a person is conducting criminal acts by using the bank account/accounts and/or for tracing/identification of the property subject to confiscation, a prosecutor with the approval of the Chief Prosecutor or Deputy Chief Prosecutor is authorised to submit a motion to a court to issue a decision on the monitoring of the targeted bank accounts. Based on the court's decision, the bank is obliged to cooperate with the investigation and to provide to it on-going information concerning transactions on one or more bank accounts. The information should be submitted by the financial intermediary to the body conducting the investigation immediately after the transaction is completed. The information concerning transfer and/or withdrawal of money from bank accounts should be provided to the investigating body prior to the completion of the banking operation. The time frame for monitoring of bank accounts shall not exceed the necessary term for collection of evidence on a criminal case.

18. In most cases, the legal document providing LEAs with power to monitor bank accounts is the Criminal Procedure Code. Unlike the postponement, which is considered an administrative act, the monitoring of bank accounts falls under the scope of the criminal procedure.
19. The factors that usually trigger the use of the LEAs' power to monitor bank accounts are: a request from a foreign authority (including FIUs), an internal analysis, a STR received from a RE or a request from the Prosecutor's office.
20. Most of the monitoring procedures are related to criminal investigations. This is the reason why bank secrecy can be overcome upon decision of the court or prosecutor, as presented below.

**BOX 19****Czech Republic**

In criminal proceedings, a public prosecutor or judge may request data protected by bank secrecy, including the monitoring of bank accounts.

**Slovenia**

The monitoring order is issued by the investigative judge upon a properly reasoned proposal of the public prosecutor; a written initiative to the public prosecutor can be, and usually is, issued by the police.

21. The survey indicates that, in most countries, bank accounts cannot be monitored at the request of institutions other than the ones included in the judicial system. In some countries, the monitoring procedure is supervised and ordered only by the judicial authorities. In these cases, LEAs are just executing orders; in other countries, the decision is made by the head of the agency (for example in Lithuania).
22. Monitoring orders must be issued in a written form, except in Lithuania where in case of emergency it can be issued orally for 24 hours. Minimum and maximum durations for monitoring orders (respectively 3 months and one year) are provided in some countries. In other countries, there are no time limitations for monitoring orders (e.g. the Czech Republic).
23. Clients must not be informed of the monitoring procedure but not all countries provide for sanctions in case of disclosure.
24. The external oversight or review of LEAs' decisions to issue a monitoring order is not compulsory in all countries. In some countries, the supervision is done within the judicial system. In others, such as the Czech Republic and Slovenia, such a mechanism does not exist.
25. In the Czech Republic and Slovenia, there are mechanisms for redress when LEAs issue a monitoring order that does not lead to a prosecution but results in identifiable losses to the person conducting the transaction or to the owner of the account. In essence, this is a civil procedure and is provided by the civil legislation. In other countries, there are no such mechanisms. However, there are mechanisms for protection of LEA employees from civil liability for any losses suffered by the subject(s) of monitoring decisions. Some systems are more orientated towards the protection of the rights of the owner of the monitored account and bank secrecy, while other systems emphasise the protection of LEAs employees engaged in monitoring procedures. Nevertheless, the survey revealed that, in general, the monitoring process does not generate losses to the individuals involved.
26. The monitoring can be triggered by a request from a foreign authority (in most cases an LEA) and such a request can also be sent to any foreign authority.
27. The survey indicated that LEAs suffer from a lack of guidelines and methodological documents to assist officers in making their analysis in relation to the monitoring of bank accounts. This was considered as a serious shortcoming since LEA officers usually have a legal background and are insufficiently trained in financial matters. Case-by-case assistance from financial experts would be another option to overcome this deficiency.
28. The manner of requesting the monitoring of bank accounts is not uniform at the national level. Various LEAs use various forms to define the information they need and the survey reveals that a standardised form might simplify and speed up the process. On the occasion of monitoring requests, the authorities of some jurisdictions meet with the private sector to organise the monitoring strategy.

29. The power to monitor banks accounts seems to be positively perceived by LEAs (considered as a privilege), but the low level of replies to the questionnaires suggests that this tool is still not routinely used by FIUs and LEAs, even though, for those countries that use it, it is considered as highly effective for AML/CFT activities.
30. Analysing the relation between the monitoring of bank accounts and postponement of the transactions, opinions were expressed that monitoring orders could be a first step before postponement, in order to increase effectiveness.

### 4.3. Monitoring of bank accounts – the private sector’s view

31. From the banks’ perspective, the monitoring process can either be an internally decided procedure or a process conducted at the request of a competent authority. Banks conduct monitoring of a client’s accounts for on-going CDD measures purposes or when ML/FT suspicion arises according to the AML/CFT national legislation and their internal rules. Banks consider the monitoring process as an essential component of the detection of suspicious activities, and automatised systems are generally in place for these purposes. The same systems are used in case of monitoring requests (orders) received from competent authorities.
32. Banks responses to the questionnaire showed that the monitoring of bank accounts is subject to different sets of rules: the AML/CFT law (Serbia and Slovenia), a special law on credit institutions (Bulgaria), and criminal proceedings laws (the Czech Republic).
33. According to the banks’ experience, monitoring of bank accounts consists of:

#### Reporting on a client’s transaction prior to its execution

Unless otherwise specified in the FIU requests, banks in Serbia report each transaction or business operation to the FIU before its completion.

#### Regular notifications within a defined timeline

In Slovenia, methods of monitoring depend on the content of requests and compliance officers provide regular feedback to the FIU in written form.

#### Applying the bank’s own practices, as developed internally for monitoring purposes

Reliance on banks’ practices can be found in the Czech Republic.

34. As a rule, banks do not provide the competent authorities with direct access to their system but the monitoring is performed by sending the information to the requiring body. Direct access to the automatic monitoring system is an exception and may be provided in Bulgaria, where either the FIU or LEA may connect themselves to the bank’s software. In those cases, the management and compliance officer is informed about the monitoring order and prepare and ensure the LEA’s access accordingly. The monitoring of the process is usually done by the compliance officer himself.
35. Most banks have systems for the monitoring of accounts as part of their IT systems used to perform obligations stipulated in the AML/CFT legislation. However, dedicated or adapted systems seem to be necessary for supporting FIU/LEA actions.
36. There are different ways the banks perform particular monitoring activities:
- Automatically
  - Semi-automatically
  - Not specialised (using software designed for other main purposes)
37. In practice, banks do not always know the indicators or the offence triggering the FIU/LEA’s request to initiate the monitoring, and only follow orders from the requesting body. The survey reveals that in cases where the private sector ignores the underlying suspicions/reasons for monitoring, the competent authority’s swift reaction is of crucial importance, particularly in case of a notification prior to the execution of the operation.
38. Unlike the postponement process, the monitoring system does not pose the same non-disclosure difficulties for the banks and the possible financial losses for the client are much

lower. There were no additional measures tabled in view of avoiding tipping-off during the monitoring procedures which could differ from recommendations on how to avoid tipping-off during postponement. Although the pressure from the client is minor in cases of monitoring, banks indicated that the non-disclosure requirements are still very important as the customers' awareness of a monitoring process would render it useless and result in the redirection of the funds to other accounts in order to circumvent it.

39. The main problem raised by the private sector is the high cost of the monitoring process. Additional costs are generated by the technical equipment necessary for the monitoring of accounts and for the communication of the results to the competent authority. The need to hire qualified additional personnel increases the costs of the monitoring process.
40. It is left to the RE to implement suitable systems for the monitoring of accounts; banks have their own IT systems used for internal monitoring but, in some cases, FIUs'/LEAs' demands require more sophistication therefore improvements and developments to systems are necessary. In the monitoring process, technical solutions are neither imposed nor provided by the authorities, making the compatibility of the systems used by private sector and FIUs/LEAs a thorny issue.
41. In some cases, technical problems render impossible the prior reporting (communication) to the authorities: transactions using new technologies or automated operations such ATM withdraws, online banking, and payments with business debit cards.
42. Another serious problem pointed-out by the private sector is related to the insufficient information received from the requesting body. Indeed, the survey revealed that, for an efficient monitoring process, the identification of the relevant transactions is extremely important. The competent authorities need to define very clearly the features of the significant transactions (sum, originator, beneficiary, explanation, country of origin...etc.), for the bank to be able to correctly detect and report those operations in the monitoring process. This is particularly important when the monitoring is imposed on bank accounts with important turn-overs.

#### **BOX 20**

##### **Slovenia**

The experience of some banks in Slovenia establishing systems for the monitoring of customer accounts on the request of the FIU revealed dependence on several factors, such as: (i) organisational structure, (ii) type of products and services provided by the bank and supported by the relevant IT system, and (iii) the number of requests received from the FIU.

43. Generally, the banks participating in the research describe the monitoring system as customer friendly. In one exception it was stated that the monitoring system has a negative impact on the bank's relationship with clients.
44. Unanimously, the private sector considers the monitoring process as effective and supporting AML/CFT efforts. It facilitates timely action by FIUs/LEAs. Also, it can be expected that, once ranked as a high-risk customer, the client will be put under enhanced due diligence scrutiny whenever he shall appear in business relations in the future. Some RE expressed the opinion that the monitoring of bank accounts system is preferable to and more effective than postponement because it provides more valuable information on STs and the parties involved.

#### 4.4. Cooperation between LEAs

45. In all countries except Republic of Moldova, an STR from a RE can be the triggering factor to start the monitoring of a bank account. In most countries, it is also possible to do it based on the FIU's own analysis. Monitoring the bank accounts based on requests from other authorities is allowed in some countries. Several FIUs can also monitor bank accounts on behalf of foreign authorities (see

46. Table 15). In Malta and Slovenia, this is not stated in law, but is done in practice.

**Table 15 Factors that can trigger the use of the FIU's power to monitor transactions – international level**

	STR from a RE	Request from the foreign FIU	Request from other foreign authority except FIU	FIU's own analysis	Request from the police	Request from the Prosecutor's office
<b>Bulgaria</b>	X	X	X		X	X
<b>Croatia</b>	X			X		
<b>Estonia</b>	X	X	X		X	X
<b>Georgia</b>	X	X		X		
<b>Latvia</b>	X			X		
<b>Malta</b>	X	X*		X		X
<b>Republic of Moldova</b>	X	X***	X***	X		
<b>Serbia</b>	X			X	X	X
<b>Slovenia</b>	X	**		X		
<b>Ukraine</b>	X	X	X	X	X	

**Note**

\* Although in Malta this is not explicitly stated in law, there is nothing in the law which precludes the FIAU from issuing a monitoring order on the basis of information provided by a foreign FIU.

\*\* There is no such direct provision in the APLMFT. However the OMLP does open cases on the base of foreign FIUs' requests and after that all the powers of OMLP could be used;

\*\*\* If it exists an agreement or international Convention

47. In practice, the monitoring of bank accounts is not extensively used, except in Serbia and Ukraine. The link with investigations, prosecutions and convictions is not strong. However, there are positive case examples.

**Table 16 Effectiveness of the monitoring**

	Monitoring orders				Investigations				Prosecutions				Convictions			
	2008	2009	2010	2011	2008	2009	2010	2011	2008	2009	2010	2011	2008	2009	2010	2011
<b>Croatia</b>	0	37	18	9		4		15			4					4
<b>Malta*</b>	N/A	N/A	N/A	6	N/A	N/A	N/A	1	N/A	N/A	N/A	0	N/A	N/A	N/A	0
<b>San Marino</b>				7				7				NA				NA
<b>Serbia</b>	97	50	88	342	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
<b>Slovenia</b>	25	0	8	9	8	0	5	3	3	0	1	0	0	0	0	0
<b>Ukraine</b>	0	0	71	134 0	0	0	1	113	0	0	1	36	0	0	0	4

**Note**

\* The legal provision enabling the issuance of monitoring orders was enacted within the second half of the year 2010, hence the N/A entries in the relative columns.

## 4.5. Conclusions

48. In general, countries consider the monitoring procedure as a valuable power in tracing illegal funds and the prevention and fight against money laundering. Especially in case of suspicion of terrorist financing, this is probably the most effective investigative instrument.
49. The monitoring of bank accounts seems to be divided between FIUs and LEAs. However, even when this power is provided by law, it appears that it is still not routinely used by FIUs and LEAs. For the countries using it, it is regarded as a highly effective instrument for AML/CFT activities.
50. The scope of monitoring powers is unevenly spread-out amongst MONEYVAL countries: for some, it applies only to ML/TF offences while others applied it to all profit-oriented crimes.
51. While in some cases the length of the monitoring time is limited (with maximum and minimum durations) the research revealed that, in general, FIUs and LEAs consider the respective duration as sufficient.
52. The factors that usually trigger the use of the LEAs' power to monitor bank accounts are: the request of a foreign authority (including FIUs), an internal analysis, an STR received from a RE or a request from the prosecutor's office. Unlike postponement, which is considered an administrative act, the monitoring of bank accounts falls under the scope of the criminal procedure.
53. The clients must not be informed of the monitoring procedure but not all countries provide for sanctions in case of disclosure.
54. The survey indicated that LEAs suffer from a lack of guidelines and methodological documents to assist officers in making their analysis in relation to the monitoring of bank accounts. This was considered as a serious shortcoming since LEA officers have a legal background and are insufficiently trained in financial matters.
55. The manner of requesting the monitoring of bank accounts is not uniform at the national level. Various LEAs use various forms to define the information they need and the survey reveals that a standardised form might simplify and speed up the process.
56. Analysing the relation between the monitoring of bank accounts and postponement of transactions, opinions were expressed that monitoring orders could be a first step before postponement, in order to increase effectiveness.
57. From the banks' perspective, the monitoring process can either be an internally decided procedure or a process conducted at the request of a competent authority. Banks consider the monitoring process as essential in the detection of suspicious activities and automatised systems are generally in place for these purposes.
58. In practice, the monitoring process is undertaken in three different forms, depending on the legislation in place and on each country's routine: reporting on a client's transaction prior to its execution, regular notifications within a defined timeline and based on banks' internal rules developed for monitoring purposes.
59. Most banks have systems for the monitoring of bank accounts as part of their IT systems used to ensure compliance with the obligations stipulated in AML/CFT legislation. However, in some instances, dedicated or adapted systems are required to support FIUs/LEAs' actions.
60. Generally, banks participating in the research consider the monitoring system as customer friendly. Unlike the postponement process, the monitoring system does not pose the same non-disclosure difficulties for the banks and potential financial losses for the client are much lower.
61. The survey revealed that cooperation between LEAs and the private sector is crucial in the monitoring process. In some jurisdictions, specific meetings are held to clearly define the case by case procedure on the implementation of each monitoring order.

### 4.5.1. Problems

62. The lack of guidelines and methodological procedures to assist the officers in the monitoring process is one of the major short-comings identified. This is worsened by the fact that monitoring has shown to be an expensive procedure and for effective application, a clear definition of the features of the transactions that are relevant is needed. The subsequent correct analysis of the money transfers registered in the bank account dramatically influences efficiency.
63. Additional costs for the REs are generated by the specific technical equipment necessary for the monitoring of accounts and by the communication of the results to the competent authority. In some instances, the hiring of dedicated trained personnel is required.
64. Another serious problem pointed out by the private sector is related to the insufficient information received from the authority ordering the monitoring. Indeed, the survey revealed that for an efficient monitoring process, the identification of the transactions which are relevant is extremely important.
65. The competent authorities need to define very clearly the features of the relevant transactions (sum, originator, beneficiary, explanation, country of origin...etc.), for the bank to be able to correctly detect and report these operations in the monitoring process. This is particularly important when the monitoring is imposed on accounts with important turn-overs.
66. New payment methods such as internet banking and the use of ATM machines render the monitoring process even more difficult, especially in cases where previous reporting to the FIU is required.
67. The risk of tipping-off still exists, albeit lower than with postponement orders.

### 4.5.2. Recommendations

68. The positive experience identified in the countries that practice the monitoring mechanism lead to the conclusion that the authorities should further encourage and facilitate the effective use by FIUs and LEAs power to monitor transactions. Awareness raising programmes to promote this tool will increase effectiveness.
69. Documented monitoring procedures should be developed by jurisdictions, clearly describing the process. Compulsory pre-meetings between FIUs/LEAs and the private sector should be included in such procedures at the beginning of the monitoring process.
70. Templates for monitoring orders could speed up the process and ensure that the RE receives all the necessary information on the transactions that are relevant for the monitoring process. It is understood that the LEA might not be in possession of all the details of possible developments related to the account, however when information is available, it should be communicated to the RE, most notably:
  - approximate sum (or thresholds);
  - features of possible payer;
  - features of possible beneficiary;
  - possible countries of origin/destination of the funds;
  - types of transactions that should be blocked or postponed (for instance all out-goings above a certain threshold);
  - type of justification provided for the transfers;
71. LEA officers should benefit from training on financial matters that are relevant for the monitoring of bank accounts and a clear methodology should be adopted to assist them in the monitoring process. The case-by-case assistance from financial experts would be another option to overcome this deficiency.
72. In order to minimise the risk of tipping-off, such behaviour should be penalised in all cases.

## 5. ANNEX – CASES

### Case 1 - Bulgaria

73. The Bulgarian FIU received an STR from a Bulgarian bank containing the following information:
74. In 2010, a Bulgarian company "S Ltd." opened two bank accounts in EUR and in BGN. For two months the turnover accumulated on the account in EUR is more than €100,000. Most of the bank operations are incoming transfers from companies registered in country A and country B.
75. A few weeks later the reporting bank received an e-mail from the managing director of "G Ltd". "G Ltd" is foreign company acting in the field of internet payments (Payment Solution Provider).
76. The information provided in the abovementioned e-mail was that "S Ltd" was engaged in criminal activity connected to the distribution of pharmaceuticals without license. The Bulgarian FIU received information that "S Ltd" used services provided by "G Ltd." via straw men. The beneficial owner and managing director of "S Ltd" was a Bulgarian national K. The Bulgarian FIU possessed information that the illegal activity of "S Ltd" was connected to selling of pharmaceuticals without license.
77. After additional verifications it was established that there were criminal records for K for embezzlement on a particularly large scale. Between 2003 and 2008, K had been prohibited from leaving the country.
78. Information was received that the activity of "G Ltd." was verified by the local law enforcement and the bank accounts of the company were frozen by the Prosecutor from country A.
79. Based on the abovementioned information the Bulgarian FIU notified the bank to put on special monitoring the bank accounts of "S Ltd" in order to provide the FIU with information about any kind of activity on these account in order to suspend future operations or deals.
80. A few days later, two wire transfers were received on one of the bank accounts S. These two transfers were ordered by two foreign companies. The transfers were in the amount of \$20,500 and €13,000. Based on the abovementioned information, these two transfers were suspended for 3 working days by the Minister of Finance. The whole of the information was sent to Prosecutor's Office.
81. Four days later K ordered another 2 payments with beneficiaries in two foreign companies. The amounts of the transfers were €29,165 and €10,000 EUR. The abovementioned transfers were also suspended for 3 working days by Minister of Finance. Subsequently, the Prosecutor's office froze the funds and an investigation commenced.

### Case 2 – Cyprus

82. A Cypriot national sent a forged money transfer order to a Bank in country X regarding the transfer of €3,000,000 from a foreign company's account to an account maintained by a Cypriot company, in a Cypriot Bank the suspect being the sole owner of this company.
83. When the foreign company noticed the transfer, they communicated with the bank and after discovering that the money transfer order was forged, they notified the Police. At the same time, the foreign bank contacted the bank in Cyprus requesting for the funds to be returned. The Cypriot bank immediately reported to MOKAS all the facts.
84. The next day an e-mail was sent to MOKAS from the foreign country's FIU, informing about the case and the facts. The foreign FIU was also informed that a formal rogatory Letter from the Judicial Authorities would soon follow so as to make it possible for MOKAS to freeze the €3,000,000 euro in the bank account in Cyprus.
85. As a result of the above information, MOKAS issued an administrative order forbidding the Cypriot bank to allow the execution of any transactions regarding the €3,000,000 in the account.
86. The formal Rogatory Letter was sent for the freezing the €3,000,000 in the Cypriot bank account together with all necessary documents required to issue a freezing order in Cyprus. The documents included a signed declaration by the person referred to as the 'purchaser' on the

sale contract provided to the Cypriot bank by the suspect. This person was actually the owner of the foreign company which had been deceived. In his declaration he claimed that he never signed a sale contract with the suspect and furthermore that he was not even acquainted with him.

87. Following enquiries with the Land Registry of Cyprus about the validity of the sale contract it emerged that no such contract was ever submitted to them. Finally, the person who received the money accepted to send them back.

### Case 3 – Cyprus

88. MOKAS received 4 STRs regarding Company A and one STR regarding Company B from banking institutions in Cyprus and 1 STR from an individual from Country X regarding Company B. Companies A and B were related because they had the same beneficial owner who was from Country Z. Companies A and B were registered in another country, their business address was in Country W and their principal activity was the IT consultancy, programming and development.
89. Based on information obtained by MOKAS, complainants informed the banking institutions that were defrauded by an investment company which tried to persuade them to invest in shares and to send the funds of the investments in Companies A and B in Cyprus. Thus, suspicions were raised due to the fact that the declared principal activity was not in line with the actual transactions i.e. the sale of shares and complainants were requesting their funds back.
90. MOKAS sent a request for information to the FIU of Country Z, the country from where the beneficial owner was. Requests for information were sent to the FIU of Country W, the country where the business address of Companies A and B were. MOKAS also informed the Cyprus Securities and Exchange Commission about the actions of Companies A and B.
91. MOKAS sent a request to all banking institutions in Cyprus in order to be informed whether Companies A and B were holding bank accounts. MOKAS informed the Authorities of Country X, about the complainant. Two administrative orders of postponement of transactions were issued to 2 banking institutions in Cyprus regarding Companies A and B's bank accounts, upon receipt of the Formal Letter of Request from Country X for a total of \$92,537.
92. Country X sent a formal letter of request and freezing orders affecting the bank accounts of Companies A and B totalling to \$99,385 were issued.

### Case 4 – Croatia

93. The Anti-Money Laundering Office (AMLO) opened a case on the basis of an STR received from a bank. The STR revealed 21 non-cash transactions with a purpose of capital increase concerning 21 companies in total amount of €14,420,000 conducted in 1 day by one natural person. All companies have the same headquarters address and the same 3 natural persons who are members of the boards of those companies.
94. After analytical processing AMLO sent a case referral to competent authorities with a suspicion on fictitious capital increase for those 21 companies mentioned in the STR, with an additional case referral which consisted of the financial intelligence analysis of financial information (bank data) on the natural person mentioned in the STR.
95. AMLO analysis also revealed that the same companies mentioned in the STR bought real estate from a number of different natural persons.
96. Further proceedings of competent authorities revealed that several natural persons were involved in illegal activities connected with overpaying in purchasing real estates. Overpaid amounts were withdrawn in cash and then deposited on the accounts of suspect persons.
97. AMLO issued a written order to three banks for the monitoring of bank accounts concerning 13 natural persons.
98. In the course of further proceedings, AMLO issued a written order to the bank for temporary suspension of a suspicious transaction execution for 72 hours for two transactions (of one natural person) in amount of app €1,110,000. In the course of this case AMLO intensively cooperated with competent authorities on inter-institutional and international level.
99. The following features of the case were identified:

- Unusual increase of capital through large number of transactions for a large number of companies conducted by the same natural person;
- Withdrawals of large amounts of cash and immediate depositing of cash in the accounts of the same or different natural persons;
- Suspicion on unreported cross-border cash transport;
- Use of accounts of other persons connected through family relations;

100. Following the FIU analysis, the prosecutor conducted an investigation against nine suspects for abuse of power and official authority and money laundering. The Court issued an order for seizure of assets belonging to the suspects (real estates, vehicles, shares, etc.), and the execution of financial transactions were temporary suspended in total value of €5,245,000.

## Case 5 – Croatia

101. Due to the suspicion on criminal offence of abuse of powers, abuse of authority in business activities, and money laundering, the specialised prosecutor on organised crime and corruption sent a request to the Anti-Money Laundering Office (AMLO) to initiate financial intelligence analysis of the mentioned transactions and persons.

102. According to the information that AMLO received from the prosecutor, company N Ltd., who was a daughter company of G Ltd., had been conducting unjustified payments in the total amount of €2,500,000 on the basis of invoices for fictitious services issued to N Ltd. by several off-shore companies.

103. AMLO sent requests for financial intelligence information to a number of foreign FIUs and in their replies AMLO received high quality information:

- Authorised persons for the accounts of the off shore companies No. 1, 2 and 3 (with the same headquarters address) were the same natural persons controlling N Ltd (Director, commercial director and former director);
- Authorised persons for the account of the offshore company No. 4 were nationals of two neighbouring countries;
- N Ltd had a non-resident account;
- The FIUs provided all the necessary bank records and forwarded financial information (bank data) for offshore company No. 5 to which N Ltd had allocated substantial funds.

104. AMLO sent requests to Croatian banks for the delivery of financial information (bank data) and received and analysed additional information from REs.

105. In the course of its financial intelligence analysis, AMLO issued a monitoring order to 6 banks concerning 5 natural persons.

106. The following features of the case were identified:

- Frequent international transfers;
- Payments to non-resident foreign accounts;
- Companies in the offshore financial centres;
- The purpose of payment – services;
- Appointees for foreign accounts were Croatian citizens;
- Case was initiated by prosecutor;
- In the course of this case AMLO intensively cooperated with competent authorities on inter-institutional and international level.

107. After the financial intelligence analysis was complete, AMLO sent a case referral to prosecutor. The prosecutor conducted the investigation and the court issued an order for seizure of assets. Total value of seized assets was approximately €3,600,000 (shares, 2 apartments, 2 houses, land).

## Case 6 – Latvia

108. The FIU received STRs from a Latvian credit institution and a sworn advocate. The reports contained information that a client of a Latvian credit institution, a company registered in Latvia, the only owner and signatory of which is a Latvian resident, was performing criminal activities. For 8 months, the Latvian company had provided wholesale trade mediation services to Eastern market companies. The services were related to international trade transactions regarding organising of the delivery of rolled metal. Essentially, those were extensive,

complicated international transactions where letters of credit issued by foreign banks were used as the payment for goods. Thus, in the period of three months, financial means to the amount of more than \$9 million were transferred to the account of the Latvian company.

109. A representative of the Latvian company informed the bank that it would buy metal from foreign companies and sells it onwards in accordance with the contracts signed with the Eastern market companies.
110. A contract signed with a foreign company was submitted to the bank. At the same time, the bank received letters of credit issued by several foreign banks in favour of the Latvian company guaranteeing the bank payments for goods delivered. Loading of freight documents as well as other documents as provided by the conditions of the letters of credit were also provided to the bank.
111. Within two months, the mentioned Latvian credit institution received at least 27 letters of credit issued by foreign banks in favour of the Latvian company. However, soon afterwards the Latvian bank started to receive information from the foreign banks that had issued the letters of credit that their clients - the purchasers of goods - had not received the goods paid for. Furthermore, the foreign clients had indicated to their banks that they were unable to contact the suppliers of goods, they had no information regarding the ships that had been designated as suppliers of freights, and the foreign company had not signed a contract with the Latvian company.
112. The FIU analysed the account statement of the Latvian company which indicated that since the account was opened it had been credited for the amount of more than \$9 million, and the origin of the funds was transactions from business partners, purchasers of metal abroad.
113. The funds had further been transferred to an account held with the same Latvian credit institution by an offshore company registered in Belize. Additionally, €40,000 was taken out in cash (possibly as a payment for the service to the owner of the Latvian company). There had been no other meaningful transactions on the mentioned account.
114. An additional information request was sent to the bank and the client explained that he was only the legal owner of the company while the company's business activity were actually being conducted by other persons who were foreigners and whose identities were unknown to him. He had only posted several advertisements on the Internet regarding selling of metal; however, any clients that responded to the advertisement he forwarded to a third person that he had never met. All the instructions he had received came via e-mail. Contracts with the business partners were signed by the third person.
115. In relation to the Latvian company and its owner, the FIU performed information searches in various state databases - Company Register, State Revenue Service Database, Property Register, and Vehicle Register. It was established that the mentioned natural person had never been engaged in business activity before, and his company was formed recently.
116. In order to prevent any further legalisation of proceeds derived from criminal activity, the FIU issued orders to suspend debit operations on the accounts of the Latvian company, for the amount of €1.4 million and on the account of the offshore company registered in Belize for the amount of \$500. Simultaneously, the FIU sent a case to the State Police, Economic Crime Enforcement Department on grounds of fraud committed on a large scale and legalisation of proceeds derived from criminal activity committed on a large scale.
117. After the case was sent to the police, the FIU received a request approved by a specially authorised prosecutor. The person directing the proceedings had received powers of attorney and applications indicating that the companies would henceforth be represented by a citizen of the Country E. The submitted powers of attorney and applications were possibly counterfeits. In order to ensure that the investigation received timely and objective information, the FIU prepared an information request to Country E's FIU which provided a reply along with a permission to disseminate the information to the police for intelligence purposes.
118. The State Police Economic Crime Enforcement Department initiated a criminal proceeding on grounds of use of counterfeit documents for purposes of illegal acquiring of property.
119. In the criminal proceedings, companies from different countries were recognised as the victims.
120. However, in the course of the investigation of the mentioned case, with the approval of the supervisory prosecutor, an independent proceeding had been separated from the main case,

since the evidence collected gave reason for considerations that the financial means were of criminal origin and of origin related to a criminal offence.

121. The proceeding on grounds of criminally acquired property was initiated due to the fact that it was not possible to submit the main case to the court in a reasonable timeframe. The circumstances of the main case were related to international cooperation, the victims were foreign companies, and possibly there were also other subjects who had performed criminal offences or joint participants. The mentioned circumstances made the process difficult and prolonged the outcome of the criminal proceeding.
122. The proceeding regarding criminally acquired property (the separate case) has been reviewed in the Court of First Instance and Court of Second Instance, as a result of which funds for the amount of €1.4 million and \$500 have been confiscated and transferred to the state budget of the Republic of Latvia.
123. It was concluded that in situations when it is not possible to submit the main criminal proceeding to the court in a reasonable timeframe, yet in order to ensure timely and economic resolve of property issues and to confiscate property, the possibility to separate an independent proceeding regarding criminally acquired property from the main case and initiate it should be used more often.

## Case 7 – Lithuania

124. The trigger for this case was Intelligence information about the fact that Lithuanian citizens acting together with associates located in foreign countries regularly carried large amounts of cash from Country P via Lithuania to Country L.
125. The Lithuanian FIU started operational activities in order to check the intelligence related to the Lithuanian citizens. Intelligence sources provided the information that the money was derived from criminal activities.
126. This information was shared with the authorities in Countries P and L. Operational activities were started by two other countries U and C in relation to the same persons. In order to effectively carry out operational activities in different countries, periodic coordination meetings were held, which resulted in the exchange of relevant information and plan further investigation.
127. The investigation finally led to the two different organised criminal groups, which operated in Countries P, G, U, C, L and Lithuania:
- holders of unaccounted cash (e.g. derived from smuggling, illegal trade of goods, etc.) targeting to introduce money into the formal financial-banking circulation and make officially the payment for the goods sold to Asia countries;
  - holders of non-cash assets targeting the obtaining of cash.
128. The main point of this modus operandi was, that cash, which is generated from trade-related crimes in different EU countries, goes not to the banking system, but into the hands of the group, which needs cash. In this case the criminal group, in need of cash gets the cash not from the bank accounts and the second group which needs to transfer illegal cash to Asia, does not place it into any bank account. This means that two invisible processes are deployed at the same time, and to detect it by monitoring bank accounts is almost impossible.
129. This criminal process is influenced by intermediaries who satisfy the interests of both groups: cash is simply exchanged to non-cash money.
130. It was found that the cash source was represented by offences relating to the import of consumer goods at very low prices in the European Union countries without the payment of the required taxes.
131. The illegal cash proceeds were transported from Countries G and C to money distribution points in Country P using couriers. Later the money passed through Lithuania to Country L (approx. €1 million per week). The total turnover of all the criminal groups was about €30 million per month.
132. In Country L, the cash was delivered to intermediaries - three separate financial groups. After receiving the cash, transfers almost equal to the sums received in cash were made from the accounts (mostly offshore) belonging to those groups in different banks to accounts in Lithuania, managed by foreign citizen W who lived in Country U. W was the organiser of "cash

exchange to non-cash” scheme. From these bank accounts, the money was transferred to offshore bank accounts for payments to suppliers of goods from Asian countries. Thus, the cash was simply exchanged to non-cash money avoiding entering it to banking sector.

133. At the same time, intermediaries in Country L were providing cash to the criminal groups for their unaccounted financial activities.
134. As stated previously, the initial phase of the operational investigation obtained data only on cash movements. When the investigation led to one offshore company account in Lithuania and analysis of transactions in this account and IP addresses was done, links with other accounts and the chain of offshore companies was established. The amount of banking information was increasing each day involving about 170 bank accounts with more than 150 thousands of financial transactions.
135. Finally, a special software tool identified the chain of offshore companies whose bank accounts had been opened in Lithuania. Transfer analysis showed the money flow from Country L to the chain accounts in Lithuania and to the Asia countries. The IP addresses showed that connections to accounts in Lithuania are mostly made from Country U and the organiser of the scheme, citizen W was identified.
136. The operation of special police and other law enforcement forces was conducted at the same time in all countries involved in May 2011. Pre-trial investigations then took place in all the countries involved. A joint investigation team (JIT) was set (supported by International Judicial Cooperation Eurojust) in order quickly and efficiently carry out the investigations.
137. All the transactions ordered in accounts in Lithuania were postponed (€4,000,000).

## Case 8 – Montenegro

138. The obligor, in this case the commercial bank, reported an STR for suspicions related to a client, a foreign citizen, who had a savings account with deposited funds for a period of one year. He required the bank to cancel the term deposit before its maturity and to pay out all the funds he had with this bank.
139. Based on publicly available sources of data, the bank found out that criminal proceedings were pending against this person in his home country due to a suspicion that he had committed a criminal offence of misuse of official position and money laundering.
140. Upon receipt of the STR, the competent administration body searched its database, it collected data, analysed them and verified the data from available sources. The database of the competent administration body recorded a higher number of cash transactions which the person in question had performed and which referred to depositing of funds, payments of cash and withdrawal of funds from the savings account.
141. At the same time, the administration contacted the foreign FIU in the jurisdiction of residence of the person in question and, following an intensive communication and correspondence, it obtained confirmation that a court proceeding was pending against this person due to a suspicion that he has committed criminal offence of misuse of official position and the criminal offence of money laundering.
142. The foreign FIU requested that the administration body to temporarily suspend execution of transactions from the account of this person. The foreign FIU also requested the Administration to make checks on whether this person had accounts opened with other banks in Montenegro. If yes, such accounts should be also be suspended temporarily. It had been disclosed in the meantime that this person had an account with another commercial bank in Montenegro.
143. The competent administration body ordered both banks to temporarily suspend execution of all transactions on these accounts for a period of 72 hours. At the same time, the information on suspicious transactions subject to temporary suspension of the execution was sent to the State Prosecutors Office and Police Directorate, and on this basis, the Prosecution Office passed a decision on extension of the suspension. At the request of the competent authorities of the client’s country of origin, his funds are still blocked.

## Case 9 – Romania

144. The FIU received a suspicious transaction report from a Romanian bank, concerning the transfer received by trading company Y (with accounts opened at bank R from O town) from

trading company X in amount of €624,300. The operation was performed through Internet banking. The transfer was justified as “consulting services”, but attached documents mentioned “dioxide carbon certificates”, although company Y’s main activity was “communications activities of cable networks”.

145. The third day after the transfer was ordered, the bank R received from a bank C (ordering bank) a request to return the amount as it was a “wrong payment”. At that time, the money was already in Y trading company’s account, and the bank could not return the money without the client’s approval. Bank R requested the client’s agreement, but the representative of company Y (Mr. J) stated in writing that he refused the refund and drew up a payment order.
146. Mr. P, trading company X’s representative, sent to bank R a copy of the penal complaint made by him against trading company Y for committing a fraud offence. From this penal complaint it resulted that the transfer in the amount of €624,300 was conducted by Mr. Z, the second associate of company X.
147. Under these conditions, bank R requested Mr. J’s (Y company representative), documents regarding source of funds. Mr. J said that he presented the invoice but the contract is confidential. From the invoice it indicated that company Y sold to company X, carbon dioxide certificates in the amount of €624,300.
148. On the fourth day, Mr. J requested a currency exchange of the amount of €624,300 in order to make the second payment to companies S and P. Bank R requested the FIU to order the postponement of the operation (the currency exchange).
149. The following resulted from the analysis performed by the FIU:
  - From accessing the database referring to the analysed persons within the FIU concluded that company S and company P have also been subject to other cases related to money laundering and tax evasion.
  - From accessing the police’s database it appeared that Mr. Z, the second associate of company X, was married to Mr. J’s sister, thus, it was assumed that there was a prior agreement between the two.
  - Under these conditions, the Office granted a postponement over a period of 48 hours and notified the General Prosecutors Office on existence of solid grounds of money laundering.
150. The conclusion was that the natural persons J and Z, on the basis of prior agreement, defrauded trading company X’s account and tried to transfer to another two companies, controlled by them, abusing the confidence of Mr. P and using fake invoices. The case is under investigation.

## Case 10 – Serbia

151. Conducting an analysis of the companies in the privatisation process from the point of view of prevention of and fight against money laundering, the Serbian Administration for the Prevention of Money Laundering (APML) noted suspicious activities carried out by a natural person XX in a short period of time (less than a year). In the analysis of data submitted by several obliged entities, the APML determined as follows:
  - XX, received cash deposits, totalling €700,000 in personal bank accounts held in a number of banks;
  - XX conducted the purchase of effective foreign currency, totalling €200,000;
  - XX made cash deposits €50,000 (in RSD) into the bank account held by a legal person Y, owned by XX; the stated purpose was “founder’s loan to the legal person”.
152. It was determined that XX acquired the legal person Y through the process of privatisation. Y’s assets consisted of non-money capital, including 250 ha of land, owned by legal person Z, in the vicinity of a main road, thus being highly marketable.
153. After the analysis of all bank accounts of the natural person XX and of the legal persons Y and Z, the APML suspected money laundering and disseminated information on XX to the competent Serbian authorities, i.e. Police and Prosecutor’s Office. The Prosecutor’s Office initiated an investigation of persons suspected to have illegally sold 250 ha of land owned by Z, which XX had previously acquired through the purchase of the legal person Y.
154. It was suspected that the land was fraudulently grossly undervalued for the privatisation purposes and that there were abuses in the acquisition process. The Police arrested a number of suspects, including XX.

155. Following the arrest of XX, the APML received an STR from a bank reporting a non-cash transfer from the company Z's account to XX's account with the stated purpose of "loan repayment". Further, a natural person AA, a nominee of XX's bank account, ordered the money transfer of €700,000 (in RSD) to the account of AB, XX's spouse. She then authorised a lawyer, BB, to further transfer the funds from AB's account into the account of the Privatisation Agency, thereby disbursing the first instalment of the purchase price of a company E that was subject of the privatisation, which is the owner of dozens of hectares of highly marketable land.
156. Consequently, based on the AML/CFT Law, the APML ordered the suspension of the transaction on the grounds of suspicion on money laundering, and informed the competent state authorities, Police and the Prosecutor's Office so that they may undertake measures within their remit.
157. The lawyer BB, one of the nominees for the AB's account, attempted to force the transfer of €700,000 to the Privatisation Agency by exerting pressure on the bank officers. Regardless, the investigative judge ordered the seizure of proceeds.
158. The procedure is still in progress, while the proceeds, €700,000, a number of condominiums in Belgrade and several hundreds of hectares of land have been seized, pending the final court decision.

### Case 11 – Ukraine

159. The State Financial Monitoring Service of Ukraine (FIU of Ukraine) received a report on financial transaction conducted by means of fraudulent actions from a banking institution.
160. Under the bank's report, there was a transfer of \$0,99 million (equivalent to UAH 7,9 million) from a USA company P through a correspondent bank (in the USA) to the account of the individual, resident A, opened in a banking institution of Ukraine with the purpose of payment of "salary".
161. The FIU of Ukraine carried out analysis of the information from the available databases of the State Tax Service and the Ministry of Interior regarding individual A and forwarded additional requests to the banking institution of Ukraine.
162. The FIU of Ukraine found out that the financial state of individual A did not correspond with the financial transactions conducted under the account. This individual lived in a dormitory, worked as a waitress and had an average monthly income of UAH 3,000 (equivalent to the \$380).
163. The FIU of Ukraine took a decision to freeze debit transactions under the account of individual A for 5 and 7 days. The amount of the funds frozen on the account was \$0,99 million (equivalent to UAH 7,9 million).
164. Moreover, the FIU of Ukraine received two official requests from the foreign country's FIU, concerning a further freezing of funds under the account of individual, resident A, for a period of 90 and 180 days, according to which the FIU of Ukraine issued the appropriate orders to the banking institution of Ukraine.
165. The unauthorised writing-off foreign funds from the account of the foreign company P, under the information obtained from the foreign FIU, was made by means of interference with the operation of the company P employee's computer during his attempted access to the banking account of the company.
166. Under the results of investigation conducted, the FIU of Ukraine prepared and forwarded the case referrals to the law enforcement agencies.
167. Under the court ruling of Ukraine, the funds from the account of individual A to the amount of the \$ 0.99 million were returned to the company P.



[www.coe.int/moneyval](http://www.coe.int/moneyval)