Financial Action Task Force

Groupe d'action financière

SECOND MUTUAL EVALUATION REPORT
ANTI-MONEY LAUNDERING AND
COMBATING THE FINANCING OF TERRORISM

RUSSIAN FEDERATION

20 JUNE 2008

TABLE OF CONTENTS

PREFACE - INFORMATION AND METHODOLOGY USED FOR THE EVALUATION OF THE RUSSIAN FEDERATION

1. The evaluation of the anti-money laundering (AML) and combating the financing of terrorism (CFT) regime of this country[1] was based on the Forty Recommendations 2003 and the Nine Special Recommendations on Terrorist Financing 2001 of the Financial Action Task Force (FATF), and was prepared using the AML/CFT Methodology 2004[2]. The evaluation was based on the laws, regulations and other materials supplied (Annex 3) by Russia[3], and information obtained by the evaluation team during its on-site visits to Russia from 24 September to 2 October and 12 to 23 November 2007, and subsequently. During the on-site the evaluation team met with officials and representatives of relevant Russian government agencies and the private sector. A list of the bodies met is set out in Annex 2 to the mutual evaluation report.

2. This was a joint evaluation of the FATF, the Eurasian Group (EAG) and the MONEYVAL Committee of the Council of Europe (MONEYVAL). The evaluation was conducted by an evaluation team which consisted of experts from the FATF, EAG and MONEYVAL in criminal law, law enforcement and regulatory issues. The team was led by Mr. Vincent Schmoll (Principal Administrator of the FATF Secretariat), Mr. Igor Nebyvaev (Principal Administrator of the EAG Secretariat), Ms. Kirsten Mandrup (Administrator of the MONEYVAL Secretariat), and further included: Mr. Richard Berkhout (Administrator of the FATF Secretariat); Ms. Colleen Stack (Assistant Director for Terrorism Finance and Financial Crime, Department of the Treasury, United States) who participated as financial expert for the FATF, Mr. Ian Matthews (Technical Specialist, Financial Crime Policy Unit, Financial Services Authority, United Kingdom) who participated as financial expert for the FATF, Mr. Stephan Ochsner (Chief Executive Officer, Financial Markets Authority, Liechtenstein) who participated as financial expert for MONEYVAL, Mr. Vladimir Gerasimovich (Expert, Department of Financial Monitoring, Belarus) who participated as legal expert for the EAG, Mr. Paul Saint-Denis (Senior Counsel, Department of Justice, Canada) who participated as legal expert for the FATF, Ms. Paula Lavric (Senior Member of the Board of the National Office for the Prevention and Combating of money laundering, Romania) who participated as law enforcement expert for MONEYVAL, and Mr. Eric Noordhoek (National Public Prosecutor for money laundering and financing of terrorism at the National Public Prosecutors Office, the Netherlands) who participated as law enforcement expert for the FATF. The experts reviewed the institutional framework, the relevant AML/CFT Laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions (FI) and designated non-financial businesses and professions (DNFBP), as well as examining the capacity, the implementation and the effectiveness of all these systems.

3. This report provides a summary of the AML/CFT measures in place in Russia as at the date of the on-site visit or immediately thereafter. It describes and analyses those measures, sets out Russia's levels of compliance with the FATF 40+9 Recommendations (see Table 1), and provides recommendations on how certain aspects of the system could be strengthened (see Table 2).

1 In all FATF Publications, all references to country apply equally to territories or jurisdictions.
2 As updated in June 2007.
3 In this report, Russia denotes the Russian Federation.

4. The evaluators would like to express their gratitude to the Russian authorities, especially to the staff at Rosfinmonitoring headquarters in Moscow and the regional offices of Rosfinmonitoring in Nizhniy Novgorod, Khabarovsk, Kaliningrad[4] and Rostov-na-Donu for their excellent assistance throughout a logistically challenging, but very well organised assessment mission.

[4] The region of Kaliningrad is part of the North-Western Federal District, which means that the regional office of Rosfinmonitoring in Saint Petersburg is responsible for Kaliningrad.

EXECUTIVE SUMMARY

Background Information

1. This report summarises the anti-money laundering (AML)/combating the financing of terrorism (CFT) measures in place in the Russian Federation as of the time of the on-site visits (25 September – 2 October 2007 and 12 – 23 November 2007) and shortly thereafter. The report describes and analyses those measures and provides recommendations on how certain aspects of the system could be strengthened. It also sets out the levels of compliance of the Russian Federation with the Financial Action Task Force (FATF) 40+9 Recommendations (see the attached table on the Ratings of Compliance with the FATF Recommendations).

2. The Russian authorities are well aware of the money laundering (ML) and terrorist financing (TF) schemes used in Russia. Many ML schemes involve the misuse of (foreign) legal entities and financial institutions. Laundered money is often invested in real estate or security instruments, or used to buy luxury consumer goods. Russia has been a repeated victim of terrorism, and the authorities report the use of TF schemes involving the misuse of alternative remittance networks by foreign and North Caucasian terrorist groups.

3. A general impediment to the fight against ML/TF is the high level of corruption in the public and private sector. There are no indications that the FIU is affected by corruption, but some law enforcement bodies and private sector businesses are impacted by corruption in varying degrees. The current and previous President of Russia have rightfully established eliminating corruption as a priority for the Russian Government.

Legal System and Related Institutional Measures

4. Russia has criminalised ML through articles 174 of the Criminal Code (CC) (money laundering), 174.1 CC (self-laundering) and 175 CC (acquisition or sale of property obtained by crime). Article 174 CC defines money laundering as an act that involves the carrying out of financial operations and other transactions with monetary funds or property knowingly acquired by other people by criminal means in order to impart legitimacy to their ownership and to conceal the criminal origin of the property. Article 175 CC states that the acquisition or sale of property knowingly obtained in a criminal manner is a punishable offence.

5. The money laundering offence extends to any property and monetary funds. It is not necessary to convict a person of a predicate offence to prove that property is the proceeds of crime. All crimes are predicate offences for ML, with the exception of 6 financial crimes. The absence of these offences could have a negative effect on the overall effectiveness the criminalisation of ML. For the predicate offences that should be covered by the ML offence, 19 of the 20 predicate offences for money laundering required under the FATF Recommendations are covered. The offences dealing with insider trading and stock market manipulation are not distinct criminal offences, although elements could be found in some other laws.

6. Only a natural person is subject to criminal responsibility, and the Russian authorities argued unsuccessfully that this principle constitutes a fundamental principle of the Russian criminal law. Notwithstanding, the Russian law provides for corporate and administrative liability for legal persons and a legal person found to have engaged in money laundering activities can have its licence revoked and ultimately be subject to liquidation through civil court proceedings.

7. There is a wide range of maximum sanctions available for money laundering by natural persons, consisting of fines (from RUB 120 000 to RUB 1 million) and terms of imprisonment (from four to 15 years). Fines can also be adjusted on the basis of the offender's income (from 0.5 to 5 times the annual income).

8. The ML offences are being increasingly prosecuted, with ML investigations jumping from 618 in 2003 to 7 957 in 2006, the number of money laundering cases sent to court going from 465 in 2003 to 6 880 in 2006 and the overall number of convictions increasing from 14 in 2003 to 532 in 2006. However, considering the level of organised crime and corruption acknowledged by the Russian authorities, the ML offence should be used even more in the future.

9. Russia criminalised terrorist financing in article 205.1 CC. The article targets any support or contribution to terrorist activity, and financing of terrorism is explicitly mentioned in the first part of the article. Criminalisation also covers the provision and collection ("raising") of funds. The financing of terrorism is connected to ten crimes of a terrorist nature, committed by both individual terrorists and terrorist organisations. However, it does not extend to the theft of nuclear material as required under the UN Convention for the Suppression of the Financing of Terrorism. Intent is required, but the Prosecution Authority does not need to prove that the funds are intended or had been intended to finance a specific terrorist act. Terrorist financing is committed as soon as the funds are collected, regardless of whether or not the funds are used in the commission of a terrorist act. The possible sentence for TF is from four to eight years imprisonment. If the same crime is committed by a person through the abuse of his office, the possible sentence is seven to 15 years imprisonment. In this last case, the judge may add a fine to the prison sentence (a maximum of RUB 1 million or five years annual income). The TF offences have been used with 24 persons convicted for the period 2004 – 2006. The average prison sentence was about eight years. Given the level of terrorist activity in Russia, the low number of cases and convictions suggests that the Russian terrorist financing provision could be used more effectively.

10. Russia possesses a dual procedure for dealing with confiscation. The Code of Criminal Procedure (CCP) and Criminal Code both contain provisions that authorise the confiscation of proceeds of crime. Article 81 CCP permits the confiscation of proceeds that are derived directly or indirectly from the commission of an offence, including income and property resulting from proceeds that have been changed to another form. Article 104.1 CC allows for the confiscation of property that is derived directly or indirectly from the commission of crime, including income and property resulting from proceeds that have been changed to another form. Both articles allow for the confiscation of instruments, equipment or other means of committing an offence or intended to be used to commit a crime. Bona fide third party rights are protected by article 123 CCP and article 169 Civil Code provides that any transaction contrary to the fundamentals of law and order or to morality is void.

11. Russian authorities have made good use of the provision under article 81 CCP as evidenced by the value of confiscation for the ML offences at over RUB 385 million in 2006 and by confiscations for all crimes totalling over RUB 75 billion from 2003 to 2006. The procedure under CC articles 104.1 has only been in effect since 1 January 2007, and so it is difficult to evaluate its effectiveness. The new provision should be easier to use and should be even more effective in targeting proceeds of crime.

12. Russia has established a system for freezing terrorist assets to comply with UNSCR 1267(1999), UNSCR 1373(2001) and successor resolutions. Russia has issued a list of designated terrorist entities with an international part (UNSCR 1267) and a domestic part (UNSCR 1373). All assets of terrorists and terrorist organisations listed in UNSCR 1267, as well as all assets belonging to persons and organisations owned or controlled by them, are frozen without time limitation or until there is a de-listing by the UN. However, no funds have been frozen so far.

13. For the domestic list (UNSCR 1373), a different regime has been created. The domestic list includes the names of entities that are identified and designated by the Russian authorities in accordance with the AML/CFT Law and the Terrorist Financing Regulation. The effect of being listed is a temporary suspension of financial operations (freezing) in respect of all assets owned or controlled by the listed entity. The freezing is reported to Rosfinmonitoring. This suspension is in effect for an initial two working days, during which time Russian authorities verify the basis for the freezing action. The freeze can be extended for an additional five working days if required in order to complete the verification. Thereafter, the criminal (seizure and confiscation) regime applies if necessary.

14. While the freezing mechanisms in the approach taken by the Russian Federation are in line with the UN Resolutions, there are elements associated with Special Recommendation III that are either absent or incomplete. In implementing UNSCR 1373, Russia relies heavily on the criminal justice system for covering the various elements contained in SR.III. Reliance on the criminal justice system risks creating problems regarding the efficient implementation of this Recommendation. For example, difficulties or delays in obtaining sufficient evidence to prosecute or convict may result in a terrorist being acquitted and his funds unfrozen. Such a result would frustrate the objectives of UNSCR 1373. In addition, Russia needs to implement an appropriate mechanism that will enable it to examine and give effect to actions initiated under the freezing mechanisms of other jurisdictions.

15. Rosfinmonitoring, the FIU of the Russian Federation, is the cornerstone of the Russian AML/CFT system. It is the central (policy) co-ordinating body for AML/CFT issues and is designated as the authority for collecting, processing, analysing and disseminating STRs. It is empowered to request information from reporting and government entities, maintain the national AML database, act as the international AML/CFT point of contact for Russia and represent Russia in international bodies such as FATF, MONEYVAL, EAG and the Egmont Group. Rosfinmonitoring was also the force that inspired the Eurasian countries to establish an FATF-style regional body, the EAG, in 2004.

16. Rosfinmonitoring has regional offices in all Federal Districts, and the co-operation between the headquarters and the regional offices seems to be good. The headquarters has established a sophisticated information technology infrastructure that enables the regional offices to analyse STRs, use the national AML database and submit cases for dissemination to headquarters. Rosfinmonitoring demands high professional standards of its employees, and internal control systems are used to protect information from unauthorised access by staff. The IT systems are designed to handle a large number of STRs and other reports. The only shortcoming detected by the evaluation team was the rather high number of staff vacancies (about 15% of maximum staff levels), especially in the analytical and supervisory departments, and the authorities are encouraged to fill all current vacancies.

17. The traditional tasks of an FIU (receiving, analysing and disseminating STRs) are performed effectively by Rosfinmonitoring, as are other important tasks that are unique to the agency, such as international co-operation and related activities such as training provided by its "*ANO Training Centre*".

18. The main law enforcement bodies involved with the fight against ML and TF are the Ministry of Internal Affairs (MIA), the Federal Security Service (FSB), the Federal Service for the Control of Narcotics Circulation (FSKN) and the Prosecution Authority. All bodies co-operate with the FIU, but it is not always clear how they co-operate with each other. The MIA, FSKN, FSB and Prosecution Authority are all clearly responsible for AML/CFT investigations, and the law designates the Prosecution Authority for delineating responsibilities for investigations when more than one body is involved. However, in practice and in all regions, there seems to be a lack of awareness by the Prosecution Authority and a lack of co-operation with the Prosecution Authority by other law enforcement bodies. This factor, along with the existence of corruption within law enforcement as acknowledged by Russian authorities, has a negative impact on the effectiveness of the system.

19. Regarding Special Recommendation IX, Russia has added AML/CFT-related requirements to its existing currency control system. The outcome is a rather confusing legal framework that appears to be interpreted differently by the Customs authorities in each of the regions visited. In practice, the effort focuses almost exclusively on cash, is not implemented as foreseen by the law, and has enforcement, legal and implementation gaps in specific areas. In addition, few sanctions for non-compliance with the declaration requirements have been levied, statistics are lacking, and Customs authorities appear to lack a clear awareness of AML/CFT measures. A full review and subsequent integration of the currency control system into the AML/CFT Law is necessary, as the physical movement of cash in and out of Russia is an important component of money laundering schemes detected in Russia.

Preventive measures - Financial Institutions (FIs)

20. The legal framework for customer due diligence is set out in a variety of legal documents. Except for the detailed provisions of the AML/CFT Law, all of these constitute other enforceable means. All financial institutions (as defined by the FATF Recommendations) are covered by the AML/CFT law.

21. Credit Institutions are explicitly prohibited from opening anonymous accounts, but there is no specific provision that prohibits banks from maintaining existing accounts under fictitious names, although the authorities believe that existing procedures effectively preclude this. All customers must be identified, although there are exemptions for certain specifically defined occasional transactions below RUB 30 000, even if there is a suspicion of money laundering or terrorist financing. Foreign exchange transactions below RUB 15 000 are also exempted from CDD, but only if there is no ML/TF suspicion. Financial institutions are in fact prohibited from performing CDD in these cases.

22. The CDD framework includes provisions on authorised persons, representatives and beneficiaries, but it does not fully address the concept of beneficial ownership. Ongoing CDD is defined as an update of CDD information, which usually must take place annually. This may not be sufficient, but it does solve possible gaps for existing customers. Financial institutions are required to assess if there are risks that make it necessary to perform enhanced CDD. There are no such rules for simplified CDD.

23. The measures against PEPs are very recent, and their effectiveness could not be assessed. However, the legal framework is incomplete and should be dealt with as a matter of urgency. Although not a strict requirement under the FATF Standards, Russia should consider including domestic PEPs as a tool for fighting corruption. In relation to correspondent banking, all of the relevant criteria should be implemented, particularly the need to understand the nature of the respondent bank's business and to ascertain whether the respondent's AML/CFT system is adequate and effective. The requirement to document the respective AML/CFT responsibilities of banks should also be covered. There seems to be no practical problem with financial secrecy provisions.

24. Record keeping requirements are generally comprehensive, but there are a few gaps in law and regulation which the assessment team recommends Russia address. Notwithstanding, the evaluation team did not receive any indication that the competent authorities had a problem obtaining required information on a timely basis. Thus, the assessment team has raised the rating for this Recommendation on the basis of effectiveness.

25. The new system governing wire transfers is a welcome step towards compliance, but gaps remain, particularly regarding the definition of originator information in certain limited cases. The assessment team recommends that the Russian authorities amend the current AML/CFT regime to address the remaining gaps and to ensure that all rules can be implemented in practice. As the legal framework for Special Recommendation VII was only implemented recently, it was impossible to measure implementation and effectiveness.

26. There is no overall requirement to examine the background and purpose of all unusual transactions and to record and maintain such information for competent authorities. Many financial institutions seem to be confused about the distinction between mandatory threshold reporting (> RUB 600 000) and examining the background of unusual transactions, however, the authorities maintain that many of the criteria for mandatory reporting are in fact unusual transactions. That said, despite the gaps in the law, in practice most FIs seem to pay attention to unusual transactions to be able to report STRs.

27. Russia bases its implementation of Recommendation 21 on the FATF list of Non Co-operative Countries or Territories, which is by itself insufficient to meet the requirements of this Recommendation. Nevertheless, Russia indicated that the Law on Special Economic Measures enables Russia to apply countermeasures in accordance with Recommendation 21, including when the FATF should decide to apply countermeasures.

28. The Russian AML/CFT Law requires the reporting of suspicious transactions in ML and TF cases, except for attempted transactions by occasional customers. While the banking sector files most STRs, other sectors also show an increase in the number of STRs. Other than these points, the shortcomings for Recommendation 13 are mostly technical.

29. Given the absence of any TF STR guidance, the authorities explained that, in practice, often a transfer of a small amount of money from a region with supposed TF activities or a withdrawal of a small amount of money from an ATM in such a region triggers an STR without any "real" TF suspicion. In addition, neither the authorities nor the private sector could indicate what the characteristics of a TF related STR would be. All of this has an impact on the effectiveness in assessing Special Recommendation IV.

30. General requirements for financial institutions to establish and maintain internal control procedures, policies, and controls to prevent ML and FT are laid out in the AML/CFT Law. Training programmes focus heavily on the legal requirements, but do not incorporate typologies, so employees are not adequately prepared to detect signs of ML and FT when they occur. TF requirements do not extend beyond the lists of designated terrorist entities. Employee screening procedures need to be broadened to cover all staff, including a criminal records check. The implementation of AML/CFT-related internal controls within Russia Post is lacking.

31. Russia has been criticised in past mutual AML/CFT evaluations for being vulnerable to criminal ownership of financial institutions, and some banks are in fact still believed to be owned and controlled by (suspected) criminals and their front men. The authorities also indicated their strong and longstanding desire to obtain the necessary supervisory instruments to deal with this issue. However, legislative changes have not yet addressed this clearly identified weakness, and all supervisors need more legal powers with respect to preventing criminals from controlling financial institutions.

32. Overall, the evaluators concluded that the supervision carried out by the BoR is detailed, in-depth and effective. For the FSFM and FISS, however, on average, each securities market participant is only inspected once every nine to 12 years and each insurance company is inspected only once every five to six years. The sample reports obtained from FSFM and FISS do not appear to be sufficiently detailed. ROSCOM inspects each Russia Post branch only once every six years, and the reports also appear to be superficial with regard to AML/CFT matters. Leasing companies are only inspected once every eight to thirteen years by Rosfinmonitoring.

33. Except for some limited guidance issued by Rosfinmonitoring (explanation of the law and typologies), no guidance has been issued. Not surprisingly, few of the financial institutions met with had any knowledge of what constitutes ML or TF beyond the legal requirements of the AML/CFT Law.

34. The powers of the supervisors are found in the law, although, for example, the BoR Law still limits the BoR in the number of on-site inspections it may carry out over a certain period (this limitation has already been mentioned in a previous AML/CFT assessment). Powers to compel production of records are sound in practice, although there some technical legal shortcomings.

35. The sanctioning powers, as well as the sanctions themselves, are in general completely inadequate. The BoR, the only supervisor with some sanctioning powers, indicated that their powers are too limited to effectively correct compliance shortcomings. The evaluation team fully agrees with the view of the BoR. The FSFM and FISS both disagreed with evaluators as to whether their powers were too limited, despite the fact that neither of these supervisors has any (direct) sanctioning powers at all. The statistics show that the system for sanctioning non-CI financial institutions does not work effectively, especially with respect to the FISS and ROSCOM.

36. The lack of effective financial sector supervision regarding AML/CFT is a key shortcoming. Russia has not effectively addressed repeated critical AML/CFT assessments identifying the need for improvement. It would be advisable for the FATF, MONEYVAL and EAG to monitor this area to ensure that remedial action is taken once and for all.

37. The current system for dealing with MVT service providers ensures a fairly effective oversight of legal MVT service providers, but it does not effectively address the existence of illegal alternative remittance systems (ARS) operating in Russia. Russian law enforcement bodies should place a higher priority on investigating the existence of alternative remittance systems to better assess the size and the nature of ML/TF threat posed by illegal MVT occurring within and through Russia.

Preventive Measures – Designated Non-Financial Businesses and Professions (DNFBPs)

38. Within the AML/CFT Law, Russia has set up two different regimes for designated non-financial businesses and professions (DNFBPs). The first regime focuses on financial institutions but it also includes the gaming industry, the real estate sector and dealers in precious metals and stones. The second regime applies to lawyers, notaries and accountants. This second regime is a less strict version of the system for financial institutions and the specific reporting requirements only apply to lawyers, notaries and accountants under certain conditions: *i)* if, during the course of business, the professional has any ground to assume that the aim of the operation or financial transaction is to launder money or finance terrorism and *ii)* if the information or service provided is not covered by professional secrecy provisions in relation to a limited set of activities that does not fully match the activities listed by the FATF. Russia should review the AML/CFT regime as it applies to DNFBPs and ensure that all relevant elements are addressed.

39. The requirements for lawyers, notaries and accountants are generally incomplete or not effectively implemented. All DNFBPs that the evaluation team met with had implemented the requirements in a different manner and not always in line with the law. There are as well some specific concerns relating to the effectiveness of the regime for casinos and the real estate sector.

40. Although real estate agents, casinos and dealers in precious metals and stones are covered by the general duty to report STRs, the figures for reporting raise some concerns over the effectiveness of the provisions. The numbers of STRs filed by lawyers and notaries appear to be very low, which calls into question whether the requirements under the AML/CFT Law are sufficiently publicised, understood or enforced.

41. All DNFBPs are supervised, but it is not always clear if this is (also) done specifically for AML/CFT purposes. The current system in which casinos are not licensed by a competent authority involved with AML/CFT matters is a cause for concern. Rosfinmonitoring is responsible for supervising casinos and real estate dealers. In the absence of specific information on sanctions imposed, doubts remain as to the effectiveness of the regime. The fact that the Assay Chamber lacks effective supervision powers and resources to focus on AML/CFT matters for dealers in precious

metals and stones is overwhelming. The supervision of lawyers, notaries and accountants concentrates on matters relating to professional practice and observance of federal legislation, including in theory, AML/CFT.

42. Russia is to be commended for identifying pawnshops, operational leasing companies and non-casino gambling enterprises as designated entities under the AML/CFT Law. Russia may also want to consider the ML risk posed by the proliferation of high value and luxury goods providers.

Legal Persons and Arrangements & Non-Profit Organisations

43. There are no bearer shares in Russia, nor are there any trusts or other similar legal arrangements.

44. All legal entities and individual businesses are required to register or update their registration at the moment of their establishment, reorganisation and liquidation as well as when any changes to the constituent documents are introduced. The law describes the data that have to be submitted to the registry which is maintained by the tax authorities. Information is publicly available, except for certain types of information that is only available to the state authorities. Information on beneficial ownership and control of legal persons as required by the FATF Recommendations is not registered or readily available to any state authorities.

45. According to the Russian authorities, the overwhelming majority of money laundering schemes are associated to a certain extent with "one-day" firms – commercial organisations registered under the names of non-existent persons without intention to perform any real commercial activity. The evaluators believe that the lack of information on beneficial ownership and control of legal persons in accordance with the FATF Recommendations is the root cause of the problem. The evaluators strongly believe that if there were effective procedures in place to gather and maintain such information, the problem with the "one-day" firms would be resolved to a large extent.

46. The Russian authorities have undertaken a superficial review of the NPO sector with an aim to determine its vulnerability to terrorist financing. While the Russian authorities seem to be of the view that the system in place is quite tough, most of the provisions involve basic registration provisions that are in place for all legal entities in Russia, including commercial legal entities. There is limited outreach to the NPO sector to provide guidance, but more needs to be done. The authorities should set up a more comprehensive and efficient system that focuses on real potential vulnerabilities and to share information to target abuse.

National and International Co-Operation

47. Russia appears to have mechanisms in place to review the effectiveness of its AML/CFT system, since new policy and legislative proposals are developed and implemented on an ongoing basis. However, the evaluation team also noted that the valuable findings of reports such as the National AML/CFT Strategy Paper and policy-oriented typologies reports by Rosfinmonitoring have had a rather limited effect in areas outside the control of Rosfinmonitoring, such as compliance with Recommendation 33 and Special Recommendations III and IX. While Rosfinmonitoring already has overall responsibility for the implementation of the FATF (Special) Recommendations, the evaluation team would recommend that it should also be given the necessary powers to ensure improved implementation.

48. Russia has implemented the Vienna and Palermo Conventions and almost fully implemented the Terrorist Financing convention. There are gaps in implementing UNSCRs 1267, 1373 and successor resolutions.

49. Russia is able to provide various forms of mutual legal assistance on the basis of the provisions of the CCP and the AML/CFT Law. Mutual Legal Assistance (MLA) is provided on the

basis of international agreements or on a reciprocal basis and is generally sound. Russia is party to a large number of bilateral and multilateral mutual legal assistance treaties. Recommendations 37 and 38 are fully implemented. In the course of the assessment, the team received information from FATF, MONEYVAL, EAG and members of other FSRBs that improvements were warranted in responding more expeditiously to mutual legal assistance requests. There also appears to be a stark difference in extradition practice in relation to non-CIS countries (the numbers seem unnecessarily low, perhaps indicating less co-operation in this area). Russia is however to be commended for the high number of requests to and from CIS countries. There are no issues in relation to other forms of international co-operation.

Resources and Statistics

50. Not all authorities keep quality statistics. While Russian authorities generally seem to have sufficient staff (based on the numbers provided), the number of staff specifically devoted to AML/CFT is generally too low.

MUTUAL EVALUATION REPORT

1. GENERAL

1.1 General information on Russia

1. Russia is the largest country in the world, covering a surface area of 17 075 200 square kilometres. Occupying all of northern Asia and the easternmost part of Europe, Russia shares 61 000 km of borders with 17 countries: Norway, Finland, Estonia, Latvia, Lithuania, Sweden (sea border), Poland, Belarus, Ukraine, Georgia, Azerbaijan, Kazakhstan (7 500 km), China (4 000 km) Mongolia, the Democratic People's Republic of Korea (DPRK), Japan (sea border) and the United States (sea border). Most of Russia's territory is united, the main exception being Kaliningrad, which lies between Lithuania, Poland and the Baltic Sea and which cannot be reached from Russia's main territory over land. Russia has the largest number of time zones for a single country in the world, spanning from GMT+2 (Kaliningrad) to GMT +12 (Provideniya Town). The population of Russia is 142.1 million (as of January 2007), with a population growth of -0.37 in 2006. The national language is Russian, next to many minority languages. Russia is home to as many as 160 different ethnic groups and indigenous peoples. As of the 2002 Russian census, 79.8% of the population is ethnically Russian, 3.8% Tatar, 2% Ukrainian, 1.2% Bashkir, 1.1% Chuvash, 0.9% Chechen, 0.8% Armenian, and 10.3% other. Russia is a democratic federal constitutional state with a republican government and it consists of 85 Federal Subjects united in 7 Federal Districts (as of 1 July 2007).

2. Formerly the Russian Soviet Federative Socialist Republic, a republic of the Union of Soviet Socialist Republics, Russia became independent following the dissolution of the Soviet Union in December 1991 (state sovereignty had already been proclaimed on 12 June 1990). Russia is considered the Soviet Union's successor state in diplomatic matters and is a permanent member of the United Nations Security Council (UNSC). Since its independence, Russia has worked towards creating a democratic political system and liberal market economy.

Economy

3. The change from a socialist planned economy to a free market economy since the early 1990s was not a smooth transition, but the current result is impressive. After the collapse of the Soviet Union until the mid-1990s, weak government institutions, the lack of rule of law and an uncontrolled change to a market economy structurally weakened the Russian economy. While a sound banking system is a condition for a healthy economy, the newly fragile banking system in Russia was to a large extent misused and controlled by criminals. This contributed to severe (social/) economic crises from 1991 to 1996 and again after 1998. Since this last crisis, the state has gradually regained control over the economy. The structural reforms enacted by the Russian government, together with a weaker exchange rate for the Russian Rouble (RUB) and higher prices for commodities such as oil, have increased business and investor confidence, contributing to an economic rebound and economic growth.

4. Russia's economy has grown since 1999, with growth rates ranging from 10% (2000) to 4.7% (2002). The growth rate for 2006 was 6.6%. Inflation is relatively high and it took until 2006 to realise an inflation rate below 10%. Since 2002, personal incomes have shown a real growth of more than 12% per year. The federal budget has run surpluses since 2001 and ended 2006 with a surplus of 9% of GDP. Foreign debt has decreased to 39% of GDP, mainly due to decreasing state debt (which was 9% in 2006). Nevertheless, problems still exist in the Russian economy. For real sustainable growth, structural economic reforms should be enacted to ensure that the economy will also grow in

times of lower commodity prices, which is in fact one of the economic goals of the Russian government.

5. Some significant structural reforms have been enacted, such as the completion of a new Civil Code, a new Customs Code, the introduction of laws simplifying procedures for land purchases and the creation of a competitive tax system with a flat income tax rate. As a consequence, foreign direct investment has risen from USD 14.6 billion in 2005 to an estimated USD 30 billion in 2006. The country's credit rating reached investment grade level and in 2006 Russia achieved a net foreign capital influx of USD 42 billion, due also to the lifting of currency restrictions since July 2006.

System of government

Federalism

6. Russia consists of currently 85 Federal Subjects that differ in the degree of autonomy they enjoy, depending on their status (republic, territory, oblast, autonomous oblast, autonomous region or federal city). Still, all Federal Subjects are equally represented in the upper house of the Russian parliament. Federal Subjects are subject to the federal level and its legal and policy framework. In addition, there are seven Federal Districts to ensure implementation of federal decisions in all 85 Federal Subjects. In this report, all references to the AML/CFT system concern the federal level and its laws, regulations, other enforceable means or other government rules, unless otherwise specified.

7. According to the Constitution, state power is exercised on the basis of separation of executive, legislative and judicial powers. All three branches of state power have the right of legislative initiative (the President, the Federation Council and its deputies, deputies of the State Duma, the government, legislative bodies of the Federal Subjects, the Constitutional Court, the Supreme Court and the Supreme Arbitration Court on issues within their competence).

Executive powers

8. Executive power is shared by the President, who is the head of state, and the Prime Minister (officially the "Chairman of the Government"), who is the head of government. The President is elected every four years by a direct vote of the Russian population (based on universal and equal suffrage) and cannot serve more than two consecutive terms. The Prime Minister is appointed by the President and is first-in-line to the presidency in the case of the President's death or resignation. The executive includes 16 federal ministries, 27 federal services, 16 agencies and 2 Committees. Lower regulations can also be signed by the President, the Prime Minister or his ministers.

Legislative powers

9. Legislative powers are exercised by the Federal Assembly, which consists of the lower house (State Duma, 450 deputies) and the upper house (Federation Council, 170 deputies). Legislative bodies also exist within the 85 Federal Subjects. All laws have to be approved by the State Duma and thereafter by the Federation Council. The Federation Council can veto a law, but has no right of amendment. If the Federation Council vetoes a law, the Federation Council and State Duma must form a conciliation commission to work out a final text of a law that has to be approved by both houses. Alternatively, the State Duma can also override a veto by the Federation Council with a 2/3 majority. The members of the State Duma are elected through general elections (party-list proportional representation with a threshold of 7% of the votes), the members of the Federation Council are selected by the President and subsequently confirmed by the Federal Subject that they represent.

Judicial powers

10. Judicial authority is exercised by the courts. Judges of the Constitutional Court are appointed by the Federation Council, and other judges of federal courts are appointed by the President. The Constitutional Court deals with constitutional cases, and its decisions are directly binding in the entire country. It has the right to (partially) review federal laws, upon request of the President, the State Duma or the Federation Council (on request of at least 1/5th of the deputies).

11. The Supreme Court is the highest judicial body on civil, criminal, administrative and all other cases that are within the competence of general courts. The Supreme Court also supervises general courts and issues judicial interpretations. The Supreme Arbitration Court is the highest judicial body on economic disputes. It also supervises lower arbitration courts and issues judicial interpretations.

Legal system and hierarchy of laws

12. Russia is a civil law country. The Constitution (adopted on 12 December 1993) and all other federal legislation is applicable throughout the territory of the country. International agreements signed by Russia cannot be invoked without implementation. However, if an international agreement sets norms different from those established by a national law then the norms of the international agreement are applied.

13. For FATF purposes, the hierarchy of laws in Russia is as follows: International treaties and conventions, the Constitution, constitutional laws, federal codes, federal laws and presidential decrees have the status of law or regulation. Ministerial and governmental decrees, agency regulations are other enforceable means. Below this level, there is a diverse set of government, ministerial and agency rules and recommendations, but none of these have the status of other enforceable means. Documents issued on the sub-federal level can have a status of other enforceable mean, however, the status of these documents is always second to federal documents.

14. As in other civil law countries, *stare decisis* (courts applying the same reasoning in similar previous cases) does not apply in Russia, although judges may follow earlier decisions by higher courts. The Civil Code provides for other legal principles. These are the general civil law principles, such as *lex specialis derogat generali* (a specific law overrules a general law), *lex posterior derogat priori* (a new law overrules an older law), and *lex superior derogat legi inferiori* (higher legal sources overrule lower source of law).

Transparency, good governance, ethics and measures against corruption

15. Russia has ratified, but not yet fully implemented, the United Nations Convention against Corruption and the Council of Europe Criminal Law Convention on Corruption. An interagency working group has been established by Presidential Decree[5] in order to develop proposals for the implementation of these two Conventions. Russia also participates in the Anti Corruption Network for Transition Economies of the Organisation for Economic Co-operation and Development, although it has not yet subjected itself to implementation monitoring. Russia joined the CoE Group of States against Corruption (GRECO) in 2007 and participates in the activities of the Asia-Pacific Economic Co-operation forum's anti-corruption and transparency experts' task force. On the domestic level, the Russian government has approved and implemented an administrative reform plan[6] that is also aimed at combating corruption.

16. The President has acknowledged the fact that corruption still is a problem. In his address before the Federal Assembly in 2006, the President stated that "despite all the efforts we have made,

[5] Presidential Decree no. 129 of 02.03.2007.

[6] Government Order no. 1789-r of 25.10.2005.

we have still not managed to remove one of the greatest obstacles facing our development, that of corruption." The President's statement is in line with other findings. Studies on Russia's corruption consistently describe corruption in Russia to be endemic, without indicating any sign of improvement[7]. According to public opinion in Russia in December 2005[8], the militia (police, customs, other law enforcement agencies and the traffic police) is perceived to be most corrupt sector in Russia, while courts and prosecutors come third on the list.

1.2 General Situation of Money Laundering and Financing of Terrorism

Money laundering

17. According to the Russian authorities, many money laundering schemes in Russia involve front companies ("one day firms") (legal entities set up by non-existing legal or natural persons, without the intention to ever perform any real commercial activity). Laundered money is usually invested in real estate (in Russia and abroad), security instruments (shares, stocks, securities derivatives) or used to buy luxury consumer goods, such as cars. The Russian authorities have also analysed in what form the criminal proceeds are laundered. In the majority of cases (60%) cash is used in the Russian currency (RUB)[9] or in foreign currencies. Security instruments were used in 12% of all cases, precious metals and precious stones account for 6% of all cases, and real estate and land were used in 4% of all cases. In 18% of all cases, money was laundered through other means.

18. Bank accounts and financial instruments are used in money laundering schemes, usually during the layering stage. At this stage, a large number of bank accounts are opened in the name of different persons, commercial organisations or front companies. The Russian authorities indicate that in a number of cases this would not be possible without the participation of financial institutions, who appear to be involved in money laundering schemes.

19. The Russian authorities currently distinguish among more than 120 money laundering typologies that are used in Russia. The most frequently used typologies detected by the authorities are:

- Account fraud.
- Front companies and identity fraud.
- Withdrawing or depositing cash.
- Back-to-back loans, often involving off-shore jurisdictions.
- Multiple transactions through a network of off-shore firms.
- Misuse of promissory notes of a fictitious company, presented by a foreign company for fictitious goods.
- Multiple movements of cash, within Russia and into and out of Russia.
- Reinvestment into the Russian economy of criminal proceeds taken abroad before.
- Creating legal enterprises to mix criminal proceeds with legitimate income.
- Sale of intellectual property in combination with invoice fraud.
- Disguising illegal proceeds as gains of gambling activities.

---

[7] See for example: *i)* The World Bank study "Anti Corruption in Transition 3", *ii)* Russian Analytical Digest, by University of Bremen and the Centre for Security Studies at ETH Zurich, volume 11/06, or *iii)* Transparency International Corruption Perception Index 2001 – 2003 and 2005 – 2006.

[8] *Source*: FOM, the Public Opinion Foundation (http://bd.english.fom.ru/cat/societas/corruption and http://bd.english.fom.ru/report/cat/societas/corruption/etb064708).

[9] RUB 100 = EUR 2.77 or USD 4.11 (as of Friday 23 November 2007, the last day of the second on-site mission).

Terrorist Financing

20. Over 1 600 citizens of Russia have become a victim of terrorism in Russia between 1995 and 2006. The following is an incomplete list of the main terrorist attacks that have taken place over the last few years: the Budyonnovsk hostage crisis (1995, 130 victims), bombing in Vlavikavkaz (1999, 54 victims), bombing in Buynaksk (1999, 64 victims), apartment bombings in Moscow (1999, 294 victims), bombing in Kaspiysk (2002, 43 victims), theatre hostage taking in Moscow (2002, 129 victims), truck explosion in Grozny (2002, 70 victims), truck explosion in Znamensky (2003, 59 victims), Chechnya stadium bombing (2003, 50 victims), explosion at a Moscow rock festival (2003, 15 victims), truck explosion near Mozdok hospital (2003, 50 victims), Moscow Red Square bombing (2003, 6 victims), Stavropol train bombing (2003, 46 victims), Beslan school hostage crisis (2004, 334 victims), Moscow subway bombing (2004, 40 victims), Moscow subway entrance bombing (2004, 10 victims), aircraft bombings (2004, 89 victims), attack on Nalchik government buildings (2005, 137 victims), merchandise market bombing in Moscow (2006, 13 victims) and bus explosions in the Republic of North Ossetia (2007, 4 victims)[10].

21. Considering the nature and scale of terrorism in Russia, the fight against terrorism focuses on prosecution and elimination of terrorists. Figures provided by the Russian authorities indicate that between 2004 and 2007 2 677 persons have been arrested for terrorism, while 774 other terrorists have been eliminated. The number of terrorism related sentences exceeds 15 000. Meanwhile, the number of terrorist acts is decreasing, from 404 in 2004 to 41 in 2007.

22. Much of the terrorist activity in Russia is home grown and linked to both the illegal Chechen separatist armed groups and to separate but overlapping North Caucasus-wide extremism. Additionally, there is evidence of a foreign terrorist presence in the North Caucasus with financial and ideological ties to international terrorism. Islamic NGOs, missionary centres and terrorist cells together foster the establishment of terrorist groups in Russia. These networks are financed to a certain degree through the misuse of alternative remittance networks. The authorities indicated that in 2006, eight alternative remittance networks were identified and liquidated by the FSB.

23. Russia actively supports relevant international efforts to prevent Proliferation Financing (PF)[11] by terrorists.

1.3 Overview of the Financial Sector and DNFBPs

1.3.1 Overview of the financial sector

24. The table below indicates what types of financial institutions in Russia conduct the financial activities that are specified in the Glossary of the FATF 40 Recommendations. It can also be used as a reference to link the terminology of the Glossary of the FATF 40 Recommendations with the relevant Russian terminology.

Types of financial activities to which the FATF Recommendations apply	Types of financial institutions in Russia that conduct these specified financial activities (including the legal basis for doing so)
Acceptance of deposits and other repayable funds from the public	Credit institutions which in accordance with the Banking Law obtain a licence for the right to accept monetary funds of physical persons and legal entities in deposits (for a certain term and on demand).
Lending	Credit institutions that in accordance with the Banking Law obtain a licence for the right to allocate accepted funds on its own behalf and at its own cost.

[10] Numbers of victims are estimates and, where possible, do not include casualties among terrorists.

[11] Proliferation Financing (PF) refers to a process where the proliferation of Weapons of Mass Destruction is financed.

Types of financial activities to which the FATF Recommendations apply	Types of financial institutions in Russia that conduct these specified financial activities (including the legal basis for doing so)
Financial leasing	Credit institutions in accordance with the Banking Law, leasing companies in accordance with the Financial Leasing Law.
The transfer of money or value	Credit institutions in accordance with article 5 of the Banking Law, organisations of Russia Post on the basis of the (Post) Communications Law and any legal person on the basis of article 13.1 (Banking Law).
Issuing and managing means of payment (*e.g.* credit and debit cards, cheques, travellers' cheques, money orders, bankers' drafts, electronic money)	Credit institutions in accordance with the "BoR Payment Cards Regulations".
Financial guarantees and commitments.	Credit institutions in accordance with the Banking Law.
Trading in money market instruments (cheques, bills, CDs, derivatives etc.); foreign exchange; exchange, interest rate and index instruments; transferable securities; and commodity futures trading	Credit institutions in accordance with the Banking Law. Professional participants in the securities market (brokers, dealers, managers, clearing companies, depositories, registrators, and securities trade organisers) who obtain a licence issued pursuant to the FSFM procedure established in accordance with the Stock Exchange and Trade Law, as well as the Securities Law. Organisations managing investment funds in accordance with the Investment Fund Law.
Participation in securities issues and the provision of financial services related to such issues	Professional participants in the securities market (brokers, dealers, managers, clearing companies, depositaries, holders of the securities registers, organisers of trade on the securities market) who obtain a relevant licence according to the Securities Law.
Individual and collective portfolio management	Organisations managing investment funds (share investment funds and mutual funds) or non-state pension funds on the basis of the licence issued by the authorised body (FSFM) according to the Investment Fund Law.
Safekeeping and administration of cash and liquid securities on behalf of other persons	Credit institutions with a licence issued according to the Banking Law. Professional participants in the securities market (brokers, fiduciary managers, depositaries) that obtain a licence according to the Securities Law. Organisations managing investment funds (management companies) in accordance with the Investment Fund Law.
Otherwise investing, administering or managing funds or money on behalf of other persons	Credit institutions having a licence issued according to the Banking Law.
Underwriting and placement of life insurance and other investment related insurance	Insurance companies (insurers and re-insurers) in accordance with the Insurance Law.
Money and currency exchange	Credit institutions with a Banking Law licence.

25. All 13 types of financial activity to which the FATF Recommendations apply are included in the AML/CFT framework. The AML/CFT Law defines the following eight types of financial institutions (AML/CFT Law, article 5):

Eight types of financial institutions in AML/CFT Law		
Type of institution	**For AML/CFT purposes only**	
	Supervisor / Regulator	**Registration with**
Credit institutions	Bank of Russia (BoR)	Bank of Russia (BoR)
Russia Post	ROSCOM	ROSCOM
Payment acceptance and money transfer services (article 13.1 Banking Law)	Rosfinmonitoring	Rosfinmonitoring
Securities companies	Federal Service for Financial Markets (FSFM)	Federal Service for Financial Markets (FSFM)
Insurance companies	Federal Insurance Supervision Service (FISS)	Federal Insurance Supervision Service (FISS)
Leasing companies	Rosfinmonitoring	Rosfinmonitoring
Pawnshops	Rosfinmonitoring	Rosfinmonitoring
Investment funds and non-state pension funds	Federal Service for Financial Markets (FSFM)	Federal Service for Financial Markets (FSFM)

Credit institutions

26. As of 1 October 2007, Russia had 1 149 registered credit institutions. All these operate under the provisions of the Banking Law[12] and are defined as "a licensed legal entity that in order to gain profit as the main objective of its activity has the right to conduct banking operations". Banking credit institutions have an exclusive right to accept funds from natural and legal persons, to place these funds on their own behalf and at their own expense and to open and manage bank accounts for natural and legal persons. Non-banking credit institutions have similar rights only in relation to individual banking operations, if allowed by the Bank of Russia (BoR). Only credit institutions are allowed to perform foreign exchange transactions. Credit institutions are also allowed to provide money or value transfer services (MVT). In this report, the term *credit institution* refers to the banking sector.

27. Banks are not allowed to engage in producing, trading or insurance activities, but are allowed to conduct professional activity in the securities market. Banks are registered by the BoR, in accordance with the State Business Registration Law[13] and the Banking Law. The BoR keeps a public register on all licensed banks (*Book of State Registration of Credit Institutions*) and only licensed banks are allowed to perform the activities stipulated in the Banking Law. The state is allowed to take all assets of illegal banks, and double the total assets as a fine. The banking sector has grown rapidly over the last years.

Russia Post

28. Apart from providing traditional postal services, Russia Post is also allowed to provide financial or banking services. This includes the right to deliver pensions, allowances and other targeted payments, sale of securities, accepting and delivering payments, receive utilities, goods and services payments and provide debit card, money or value transfers and ATM services. The legal basis for all services can be found in the (Post) Communications Acts[14]. The licence for all financial / banking services is renewed once a year. Although the law would not prohibit the government from granting licences to more businesses, currently only the national postal monopoly Russia Post is allowed to provide these services. Russia Post has 85 branches and approximately 42 000 offices all over Russia.

12 Federal Law no. 395-1 (02.12.1990) "On Banks and Banking Activity".

13 Federal Law "On State Registration of Legal Entities and Individual Entrepreneurs".

14 Federal Laws no. 176-FZ "On Post Communications" and no. 126-FZ "On Communications" (both 07.07.2003).

Russia Post is supervised by ROSCOM, which has issued a single licence for all activities by Russia Post, including the financial / banking services it provides.

Payment acceptance and money transfer services (article 13.1 Banking Law)

29. Certain commercial non-banking legal entities have the right to accept cash from the public and to transfer these funds to other entities (payment acceptance [приём платежей in Russian] and money transfer services)[15]. This service is allowed for the payment of telecommunication services, rent and utilities. The service can be provided without a licence and does not include the opening of an account for the customer. According to the Russian authorities, this exemption in the law was provided to legalise an existing practice, and these services are not the provider's main type of commercial activity. The relevant authorities indicated that they did not know why the parliament had decided in July 2006 to exclude part of the banking and payment system from certain provisions of the Banking Law. They indicated their dissatisfaction with this loophole and pointed at significant AML/CFT risks, even though the Parliament had decided to designate these entities under the AML/CFT Law (also July 2006). The registration regime only became effective while the evaluation team was in Russia, thus these providers had to register with Rosfinmonitoring from November 2007 (53 entities as of December 2007) and Rosfinmonitoring started to supervise the entities from that time. They are also required to have a contract with a CI that carries out the second part of the transfer within the payment system.

Securities sector

30. The Securities Law[16] distinguishes seven types of securities market activities, which as of 1 January 2007 are performed by 1 711 registered entities (brokers, dealers, managers, clearing companies, registrars, exchanges). All professional activity on the securities market must be licensed by the Federal Service for Financial Markets (FSFM). Banks can also provide securities services, as long as they have a banking licence. Overall, there are three types of licences for securities: professional licences, maintenance licences and Stock Exchange licences. The trading volume at the Russian Trading System for the first half of 2007 exceeded RUB 2 472 billion and the capitalisation of the Russian share market amounts to approximately 90% of the GDP of Russia.

Insurance sector

31. The insurance sector is regulated by the Federal Insurance Supervision Service (FISS) and governed by the Insurance Law[17]. The insurance sector in Russia includes reinsurance and mutual insurance, and all types of insurers, including life, have been designated under the AML/CFT Law. Insurers are allowed to estimate insurance risk, receive insurance premiums (insurance contributions), form insurance reserves, invest assets, define amounts of loss or damage, make insurance payments, and perform other actions connected with the discharge of insurance contracts obligations. As of 1 January 2007, 912 entities had been licensed and registered, a number that decreased to 857 by the end of 2007. The insurance sector in Russia is new and small. In 2006, the sum of insurance premiums amounted to RUB 602 million, 23% more than in 2005. At the same time, insurance payouts grew by 26% to RUB 345 million.

Leasing companies

32. Leasing companies[18] in Russia are commercial entities (resident or non-resident in Russia). The leasing company (lessor) will finance the purchase of an asset financial lease for another entity (lessee), without necessarily transferring ownership. Leasing companies were originally required to be licensed, but as of February 2002, licensing is no longer required. Currently, 912 leasing companies

15 Federal Law no. 140-FZ of 27.07.2006.
16 Federal Law no. 39-FZ "On Securities Market".
17 Federal Law no. 4015-1 of 27.11. 1992 "On Insurance Activity in Russia".
18 Federal Law no. 164-FZ "On Financial Leasing (Leasing)" of 29.10.1998.

are registered. It is not entirely clear how many leasing companies are involved in financial leasing (which is covered by the FATF definition) as opposed to operational leasing. The evaluation team was only able to meet with one leasing company, which was involved in operational leasing. Nonetheless, the AML/CFT (legal) framework for operational and financial leasing companies is identical.

Investment funds and non-state pension funds

33. Investment funds[19] and non-state pension funds have been designated under the AML/CFT Law. In the Investment Fund Law, investment funds and non-state pension funds are defined as management companies, created as an open or closed joint stock company or a limited (additional) liability company under Russian law, operating on behalf of its shareholders. Investment funds need a licence from the FSFM. Investment funds are not allowed to provide any additional services, except for fiduciary management of securities and insurance reserves of insurance companies. As of 1 January 2007, 305 investment funds have been registered.

Pawnshops

34. Russia considers pawnshops to be part of the financial sector. However, since pawnshops do not fall under the definition of a Financial Institution or Designated Non-Financial Business or Profession (DNFBP), this sector is not discussed in this report, except for section 4.4.

1.3.2 Overview of designated non-financial businesses and professions (DNFBP)

35. Russia has designated most non-financial businesses and professions (DNFBPs) listed in the Glossary of the FATF 40 Recommendations, but some of them are neither supervised nor registered in Russia for AML/CFT purposes.

FATF Designated Financial Businesses and Professions in AML/CFT Law			
Sector	**Designated / no designated**	**Effectively supervised or monitored for compliance (for AML/CFT purposes only)**	**Registered (with) (for AML/CFT purposes only)**
Casinos (including internet casinos)	Designated	Yes	Yes (FIU)
Real estate agents	Designated	Yes	Yes (FIU)
Dealers in precious metals and stones	Designated	Yes	Yes (Assay Chamber)
Lawyers	Designated	No	No
Notaries	Designated	No	No
Accountants[20]	Designated	No	No
Trust and Company Service Providers	Not designated	No	No

Casinos (including internet casinos), including other forms of gambling

36. Gambling is defined in Russia in the Tax Code, regulated by the Civil Code and includes lotteries, mutual betting and other risk-based games. Gaming providers need to be licensed; a licence is valid for five years. The Russian AML/CFT Law does not distinguish between various types of

[19] Federal Law no. 156-FZ "On Investment Funds" of 29.11.2001.

[20] The authorities did not provide information in relation to accountants before, during or just after the on-site.

gambling, however, for the FATF purposes, only casinos are discussed in this report. All other gaming is only mentioned in Section 4.4 of this report.

37. Since all gaming activity must be registered with Rosfinmonitoring, the Russian authorities know that 2 541 gaming organisations are active in Russia, of which 348 are casinos. After 1 July 2009, all gaming will be prohibited in Russia, except within 4 newly created special gaming zones in Kaliningrad, Rostov-na-Donu, Altai and Primorskiy Krai (Vladivostok).

Real estate agents

38. In Russia, real estate includes land and everything that is closely connected with land. Air and sea vehicles subject to state registration, inland water vessels and space objects are also considered to be real estate according to the law. All real estate objects must be registered; all information in this register is available to every person. Since 2001, the rules for the real estate sector have been liberalised. The only relevant requirement (for this report) for real estate agents is registration with Rosfinmonitoring. As of January 2007, 1 859 real estate agents (agencies) have been registered. The Federal Tax Service (FTS) also registers real estate businesses and shares its register with Rosfinmonitoring. The overall volume of real estate transactions rose from RUB 262 billion to RUB 691 billion between 2004 and 2006.

Dealers in precious metals and dealers in precious stones

39. Russia has set up an extensive regulatory framework for commercial handling of precious stones, metals and jewellery[21]. Over 25 000 entities that deal in precious metals and stones have registered with the Assay Chamber, of which about 13 000 carry out wholesale and retail trade that would fall within the FATF definition of this sector (accepting cash above EUR/USD 15 000). This framework has originally been set up for other reasons than AML/CFT, and AML/CFT issues are certainly not the main concern for the Assay Chamber.

Lawyers

40. At present, there are about 60 000 lawyers in Russia. Their status is protected by the Lawyers' Law and defined as qualified and professional judicial assistance provided to natural and legal persons in order to protect their rights, freedoms and interests and to provide their access to justice. Advocacy is not considered a business, but an independent professional legal activity. Lawyers cannot engage in other business activities (except for scientific, teaching or other creative activities) and cannot take state positions on any federal level. Lawyers are designated under the AML/CFT Law, however, they enjoy a separate regime.

Notaries

41. The 500 state and 7 000 private notaries provide a range of services to the public, all based on the Notary Law. Professional secrecy applies to all notaries, unless a court frees the notary to defend personal interests. All notaries can be licensed by an SRO, but not for AML/CFT purposes. Among the services provided by notaries are: issue property right certificates, authentication of documents, signatures, translations, identities, taking money or securities into deposit, handling checks and guarantee evidence. Notaries are designated under the AML/CFT Law, however, they enjoy a separate regime.

Accountants and trust and company service providers

42. Accountants are designated under the AML/CFT Law; however, they enjoy a separate regime (equal to lawyers and notaries). Accountants are in Russia referred to as auditor, and act on the basis of the Auditing law. Auditors are licensed by the MoF, but not for AML/CFT purposes.

[21] Federal Law no. 41-FZ "On Precious Metals and Precious Stones" of 26.03.1998.

43. According to the authorities, trust service providers do not exist in Russia, although nothing would prohibit any natural or legal person from providing any of the activities listed in the FATF Recommendations (and such services are advertised). The existence of company service providers was not contested and, this sector has not been designated under the AML/CFT Law. The Russian authorities did not provide any other information with respect to these sectors, nor did the evaluation team meet with any of these professions during the on-site visits. Since the FATF Recommendations do not differentiate between Trust and Company Service Providers (TCSPs), this report refers to TCSPs as a whole.

1.4 Overview of commercial laws and mechanisms governing legal persons and arrangements

44. All legal entities are defined in the Civil Code and divided into commercial and non-profit entities. All commercial legal entities need to register with the FTS, and all non-profit entities with Rosregistration (ROSREG), before assuming legal capacity. The registration procedure and the documents that legal entities need to submit to register are contained in the State Registration Act[22]. Information contained in the register is available to the public, except for bank account information of the legal entity or information on the private address of an individual entrepreneur (article 6, State Registration Act).

Commercial entities

Limited liability partnership

45. Limited liability partnerships are formed on a contractual basis, all partners are supposed to participate in the activity of the legal entity and bear (personal) liability for the company's obligations.

Limited liability company

46. A limited liability partnership is established on a contractual basis. The participants are not personally liable for the responsibilities of the company, except for their share of the (minimum) capital. The participants do not have to take part in the management of the company. The company's shares can be transferred to other parties.

Limited partnership and double limited company

47. A limited partnership combines a limited liability partnership and a limited liability company. Only partners can be part of the management and bear (personal) responsibility, investors can only lose their investments. A double limited company differs from a regular limited liability company by the fact that all investors are jointly responsible for the company's liability – and not just for their own share as with the limited liability company.

Joint stock company

48. A joint stock company is defined as a company where the authorised capital is divided into a definite number of shares (securities). These securities can only be issued by joint stock companies. The Securities Law and the Law on joint stock companies require that all securities be nominal.

Production co-operative, state-run and municipal unitary enterprises

49. Production co-operatives are alliances of labour and capital and are mostly found in the agricultural sector. State-run and municipal unitary enterprises are enterprises set up by governments.

[22] Federal Law of 08.08 2001 no. 129-FZ "on State Registration of Legal Entities and Individual Entrepreneurs".

Non-profit entities

Consumer co-operatives

50. Consumer co-operatives are voluntary associations of citizens and other legal entities, established to satisfy the needs of its participants. Participants pay a member fee.

Public and religious organisations and associations

51. Public and religious associations are defined as groups of citizens that form legal entities on the basis of their common interests or for the satisfaction of spiritual and other non-financial needs. These organisations may make a profit, but only to maintain their activities. The members of the associations cannot claim ownership of any property of the association. The law also establishes the right to form public or religious associations to members of indigenous nations (*"native smaller peoples' communities"*), on the basis of self-definition and regional neighbourhood, with the aim of protecting the local environment, the traditional way of life and culture.

Funds

52. A fund is a non-profit entity without membership, established by citizens and legal entities that pay membership fees. Funds can be established for social, charity, cultural, educational and other generally useful purposes.

Institution

53. An institution is formed by a natural, legal or public entity. The owner of the institution is liable for the finances and obligations of the institution.

Associations and unions of legal entities

54. Commercial organisations can join forces to co-ordinate their businesses, defend their (sector's) (commercial) interests and work for the public interest.

1.5 Overview of strategy to prevent money laundering and terrorist financing

1.5.a AML/CFT Strategies and Priorities

55. The national AML/CFT strategies and priorities are defined in the National AML/CFT Strategy Paper[23] (NASP). Follow up reports on the implementation of the NASP are sent annually to the Prime Minister's Office. The NASP is a policy paper that is approved by the President and includes the 5 strategic objectives indicated below.

- Limiting the scale of organised crime and illegal business activity.
- Eliminating conditions that foster terrorism, organised crime, drug trafficking and corruption.
- Preventing illegal transfer of monetary funds and income abroad.
- Recovering proceeds of crime previously illegally transferred abroad.
- Creating and ensuring efficient state bodies that participate in combating money laundering and financing of terrorism, including an optimal interagency co-ordination structure.

[23] Full translated title "Concept of national strategy on combating money laundering and terrorist financing".

56. These five strategic objectives have to be achieved along the following main lines:

- Create an effective legal basis for a well functioning AML/CFT system.
- Improve identification and customer due diligence (CDD) policies and laws by introducing user group targeted obligations, introduce risk models and map out the data needed to identify the beneficial owner.
- Improve supervisory efficiency, which includes an optimised frequency of inspections, strengthening control over supervised bodies, and gather knowledge over the structure, beneficiaries and owners of supervised entities.
- Improve the organisation of activities of Rosfinmonitoring and other bodies concerned with AML/CFT, especially in relation to material and technical support. This includes expansion of IT capabilities and the creation of a uniform information database.
- Improve of law enforcement and court performances in ML/TF cases. This includes better investigation techniques, training of qualified investigators, prosecutors and judges and the creation of a state protection programme for state employees and involved citizens.
- Enhance interagency co-ordination between Rosfinmonitoring and law enforcement bodies, law enforcement and supervisory bodies, within law enforcement bodies, among supervisory bodies, and co-operation with supervised entities. Co-ordination includes exchange of information, the development of a joint methodology to combat ML/TF, and establishment of a general procedure to set up joint working groups on all areas and on all forms of crimes.
- Strengthen international co-operation by participation in international bodies, conclusion of memoranda of understanding (MOUs), development of effective forms of co-operation between Russian agencies and their foreign counterparts, information exchange and creation of expertise in the region by providing AML/CFT assistance to other member states of the Commonwealth of Independent States (CIS) and to the Eurasian Group (EAG).
- Increase professional AML/CFT training by creating a nationwide AML/CFT training system, setting up of a training centre at Rosfinmonitoring, developing a system of follow up training for AML/CFT experts from all agencies, developing advanced AML/CFT knowledge enhancement training for prosecutors and judges, and provide language training for the Russian experts that participate in international co-operation.
- Create a system to evaluate the efficiency of the measures taken to combat ML and TF. This system should include criteria measuring quality and quantity on an academic level and be based on a complex and comprehensive data collection system.

1.5.b The institutional framework for combating money laundering and terrorist financing

Overall executive responsibility

The President

57. The President has the ultimate responsibility for all aspects of Russia's AML/CFT system. The President can, by decree, set up interagency working groups to develop policy plans that have to be approved by the President. Also, as the top executive, the President is responsible for the structure of the Russian executive branch, which includes almost all bodies concerned in AML/CFT.

The Security Council

58. The Security Council advises the President on issues of national security, which includes terrorism and money laundering. These threats can be internal or external. The Security Council is chaired by the President.

The Presidential Plenipotentiaries

59. Implementation of presidential and other federal decisions is achieved through Plenipotentiaries of the President in each of the 7 Federal Districts created in 2000. Every Federal District is made up of several Federal Subjects, on the basis of economic interdependence and territorial proximity. The 7 Federal Districts are (acronym and administrative centre within brackets): Central* (CFD, Moscow), North-West* (NWFD, Saint-Petersburg), Southern* (SFD, Rostov-na-Donu), Volga* (VFD, Nizhniy Novgorod), Ural (UFD, Yekaterinburg), Siberian (SiFD, Novosibirsk) and Far Eastern* (FEFD, Khabarovsk). Regions marked with * were visited by the evaluation team.

Federal Ministries and Executive Bodies

Rosfinmonitoring

60. Rosfinmonitoring (official full name *Federal Financial Monitoring Service*), is the Russian Financial Intelligence Unit (FIU) and co-ordinates the activities of all state bodies involved in AML/CFT issues. It was established in November 2001 within the competence of the Ministry of Finance until October 2007, when it became part of the competence of the Government, as the (office of the) Prime Minister is referred to in Russia. As an FIU, Rosfinmonitoring receives, processes and analyses information connected with ML/TF and forwards information to law enforcement bodies, if necessary. Rosfinmonitoring is also the registration and supervisory authority for leasing companies, pawnshops, real estate agents, the gambling sector and organisations according to article 13.1 Banking Law.

Ministry of Finance

61. The Ministry of Finance (MoF) combines the responsibilities for the federal budget and treasury (budget, tax, financial markets, national debt, state auditing and accounting, customs, pension funding, gambling). It co-ordinates the activities of several agencies with AML/CFT related duties that are within the competence of the Ministry, such as the FTS the FISS and the Assay Chamber.

Ministry of Justice

62. The Ministry of Justice (MoJ) is responsible for the drafting of all legislation in Russia, the protection of human and citizens' rights and freedoms, mutual legal assistance (MLA) in civil cases, implementation of international treaties, registration of foreign legal entities and extradition matters. It is also responsible for ROSREG, the supervisory body for NPOs.

Ministry of Foreign Affairs

63. The Ministry of Foreign Affairs (MFA) is the responsible authority for international relations, in order to establish a unified foreign affairs policy. The MFA is also responsible for the implementation of international agreements.

Ministry of Internal Affairs

64. The Ministry of Internal Affairs (MIA) is responsible for law enforcement and immigration issues and services. It is not just the governing body for law enforcement, the MIA is also the police. It is the responsibility of the MIA to detect, prevent, disclose, suppress and investigate crimes and administrative offences. The MIA is also concerned with public order and road traffic security issues,

and the protection of state property. The MIA is also known by its Russian acronym MVD (МВД) and by the term *militsiya* (милиция).

Federal Security Service

65. The Federal Security Service (FSB) is the Russian domestic state security and intelligence service, responsible for counterintelligence, federal border protection, anti-terrorism operations and the fight against corruption and organised crime. AML/CFT issues are well within the competence of the FSB.

Federal Service for the Control of Narcotics Circulation

66. The Federal Service for the Control of Narcotics Circulation (FSKN) is the law enforcement body authorised to control and fight all criminal matters in relation to narcotic drugs, psychotropic substances and their precursors. It is a competent body in those cases where drugs money is laundered.

Federal Customs Service

67. The Federal Customs Service (FCS) is an executive body that controls imports and exports to Russia, supervises the activities of customs, currency transactions and takes enforcement actions against smuggling, other crimes and administrative offences. The FCS has law enforcement duties and powers, executed by the Customs investigation and Customs law enforcement directorates.

Supervisory Bodies

Bank of Russia

68. The Bank of Russia (BoR) is the Central Bank of Russia. It is independent from other government bodies and only reports to the State Duma. The head of the BoR is appointed or dismissed by the President, with the approval of the State Duma. The BoR is responsible for the stability of the national currency, for the development of the banking system and for an efficient payment system. The BoR is also the regulator and supervisor for credit institutions. Some of its AML regulatory and supervisory powers are defined in the AML/CFT Law.

Federal Service for Financial Markets

69. The Federal Service for Financial Markets (FSFM) is the Russian regulator and supervisor for the securities market. One of its many tasks concerns AML/CFT supervision (securities, investment management and non-state pension funds).

Federal Insurance Supervision Service

70. The Federal Insurance Supervision Service (FISS) is the regulatory and supervisory body for the insurance sector. The FISS is subordinate to the MoF. The FISS is concerned with long-term stability and prudential issues, but it also plays a role in enforcing AML/CFT Laws. Within its AML/CFT competence, the FISS makes quarterly reports of findings to Rosfinmonitoring on supervision of insurance companies.

Roscommunication

71. Roscommunication (ROSCOM) is the supervisory body for Russia Post. Its official (translated) name is the Federal Service of Supervision in the sphere of mass communication, communication and protection of cultural heritage (*Rossvyazokhrankultura*). It is responsible for many other matters besides the compliance of Russia Post with the AML/CFT Law.

Assay Chamber

72. The Assay Chamber is also subordinate to the MoF. It is the supervisory body that controls entities' compliance with rules concerning trade in precious metals and stones, jewels (and scrap). It also controls AML/CFT duties of the supervised entities and co-ordinates its activities with Rosfinmonitoring.

Federal Registration Service

73. The Federal Registration Service (ROSREG) is the executive body responsible for registration of real estate ownership (land registry), political parties and public associations (and other related state registers) and other legal entities, except for commercial entities that register with the FTS. It is also the supervisory body for lawyers and notaries (but not for AML/CFT purposes).

Federal Tax Service

74. The Federal Tax Service (FTS) is tasked with the collection of federal taxes in Russia. It also exercises supervision over currency operations and over lotteries. The FTS is also responsible for the registration of commercial legal persons and lotteries. All its duties are carried out under the authority of the MoF.

Prosecution and Courts

Prosecution Authority

75. The Prosecution Authority is an independent, centralised authority. Its main task is to supervise the observance of all laws in Russia, including AML/CFT related laws. As with many civil law countries, the Prosecution Authority co-ordinates all law enforcement activities related to combating crime. Its main task is of course the prosecution of suspected criminals before the courts. The Prosecution Authority is headed by the Prosecutor General, who is nominated by the President and approved by the Federation Council (five year terms). The Prosecution Authority can also independently investigate criminal cases, thereby acting as any other law enforcement body. It is the central authority co-ordinating the provision of MLA on all criminal cases.

Courts

76. The three types of courts in Russia (Constitutional, General and Arbitration in economic disputes) may all be involved in cases related to AML/CFT. Most AML/CFT cases would however be channelled through the General Courts (Justices of Peace, Federal Districts Courts, High Courts and Supreme Court). The Supreme Court has the authority to suspend the activities of any commercial or non-profit legal entity.

Self Regulatory Organisations

Federal Lawyers Chamber

77. The Federal Lawyers Chamber is an NPO authorised to represent the interests of lawyers.

Federal Notarial Chamber

78. The Federal Notarial Chamber is an NPO authorised to represent the interests of notaries.

1.5.c Approach concerning risk

79. Russia has not formulated a risk-based approach to define which sectors should or should not be designated. However, Russia has mapped the risks that threaten the effectiveness of the AML/CFT system. This work was the basis for the National AML/CFT Strategy Paper (NASP).

80. The Russian AML/CFT system is based on:

- The understanding of the social, economic and financial situation, the security risk, as well as the level and nature of crime.
- The international standards, including the FATF Recommendations.
- The understanding that ML follows other crimes.
- The recognition that AML/CFT activities are fundamental to fight crime and terrorism.
- The knowledge that criminal, civil and administrative liabilities must support and enhance compliance with AML/CFT measures.
- The realisation that international co-operation in the AML/CFT area is pivotal.

81. The risks that threaten the effectiveness of the AML/CFT system and should be taken into account when developing AML/CFT measures are:

- Corruption in state bodies (including law enforcement bodies and the judicial system).
- Possibilities to hide ownership and control, by use of offshore jurisdictions by Russian businesses and other tools that enable anonymous operations and settlement.
- Use of alternative banking systems.
- Shortcomings in supervision and other control mechanisms for the financial sector which creates opportunities for illegal funds to be sent abroad.
- Lack of an efficient border control system with respect to the entry of foreigners.
- A cash-based economy.

82. The NASP itself also included a list of risks that threaten the Russian AML/CFT system and that should be taken into account when developing that system:

- Lack of information within state bodies involved in AML/CFT issues; AML/CFT data are not bundled in one place.
- Lack of trained staff within law enforcement and supervision bodies.
- Low level of money laundering and terrorist financing crimes that are detected and solved, due to low levels of training and lack of operational co-operation.
- Lack of experience with AML/CFT cases within law enforcement, prosecution and the courts.
- Gaps in the law, especially in supervisory laws that insufficiently define AML/CFT supervisory powers and lack a risk-based focus.

1.5.d Progress since the last mutual evaluations

83. This is a joint mutual evaluation by the Financial Action Task Force, the MONEYVAL Committee of the Council of Europe and the Eurasian Group.

84. This is the first mutual evaluation of Russia by the Eurasian Group.

85. This is Russia's second assessment report by the FATF. The first assessment by the FATF was based on the previous standard (the 1996 FATF 40 Recommendations). The on-site visit took place in April 2003 and the report was discussed in June 2003. The evaluation led to the decision that Russia, at that time observer to the FATF, should become a member of the FATF.

86. This is Russia's third assessment report by MONEYVAL. The on-site for the first mutual evaluation by MONEYVAL took place in June 2000, and the first mutual evaluation report was discussed in January 2001. The on-site for the second mutual evaluation by MONEYVAL took place in September 2003, and the second mutual evaluation report was discussed in July 2004. The second assessment of Russia, although undertaken in 2004 (after the 2003 revision of the FATF Recommendations), was also based on the previous 1996 FATF Recommendations.

87. To avoid duplication, Russia's progress since the first mutual evaluation of the FATF (April – June 2003) and the second mutual evaluation of MONEYVAL (September 2003 – July 2004) is described in consolidated form, based on the recommendations made in both earlier reports.

88. Russia has implemented a large number of measures in its AML/CFT regime, and this report discusses these changes in detail. The most notable changes are:

- The deletion of the threshold for the criminalisation of ML (see section 2.1).
- The Supreme Court has ruled that a prior conviction for a predicate offence is not needed for a ML conviction (see section 2.1).
- The number of convictions for money laundering has risen substantially (see section 2.1).
- The abolishment of confiscation as an additional punishment (see section 2.3).
- The regional offices of Rosfinmonitoring have now full access to the database of the headquarters (see section 2.5).

89. However, some recommendations made in 2003 and 2004 have not been followed up, and these recommendations are repeated in this report. One of these is the repeated failure to establish criminal liability for legal persons (see section 2.1). Most recommendations that still have not been implemented are discussed in section 3.10 of this report and relate to the lack of powers and resources of the supervisory bodies (BoR, FSFM, FISS and ROSCOM).

2. LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

2.1 Criminalisation of Money Laundering (R.1 & 2)

2.1.1 Description and Analysis

Recommendation 1

Criminalisation of ML on the basis of the UN Conventions

90. The Vienna and Palermo Conventions require countries to establish as a criminal offence the following intentional acts: conversion or transfer of proceeds; concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to proceeds; and the acquisition, possession or use of proceeds [Vienna article 3(1)(b) (i)–(ii) and (c) (i), and Palermo article 6(1)(a)(ii) and (b)(i)].

91. In Russia, money laundering is criminalised by articles 174 of the Criminal Code (CC)[24] (money laundering), 174.1 CC (self-laundering) and 175 CC (acquisition of property obtained by crime). Article 174 CC defines money laundering as an act that includes the completion of financial operations and other transactions with monetary funds or property knowingly acquired by other people by criminal means in order to impart legitimacy to their ownership and to conceal the criminal origin of the property**.**

92. Article 175 CC states that the acquisition or sale of property knowingly obtained in a criminal manner is a punishable offence.

93. The elements of the ML laundering offences found in articles 174, 174.1 and 175 CC are criminalised in line with the requirements of the Vienna and Palermo Conventions.

- *Conversion* or *transfer* is covered by the first sentence of the criminalisation ("Accomplishment of financial operations and other deals in monetary funds or other property"). "Financial operations" is defined in the AML/CFT Law as an action of the launderer, aimed at setting up, changing, or ending civil rights or responsibilities (article 3). "Deal" is defined as an action of a natural or legal person aimed at setting up, changing or ending civil rights or responsibilities, related to those funds or assets (article 153 Civil Code).
- *Knowledge* is covered in the first sentence of the criminalisation. The evaluators were informed that under the Russian law, this includes "should have known".
- *Concealment* or *disguising* is also covered; the language used is "for the purpose of bringing the appearance of legality to". Russian officials informed the assessors that this element of their offence was broad enough to capture activities meant to conceal or disguise the true nature, source, location, disposition and movement of proceeds where the individual is aware that the property in question is proceeds.

[24] Article 174 CC was translated as follows:
Legalisation (laundering) of funds or other property acquired by other persons through committing a crime.
1. Accomplishment of financial operations and other deals in monetary funds or other property knowingly acquired by other persons by criminal ways (except for the crimes stipulated by Articles 193, 194, 198, 199, 199.1 and 199.2 of this code), for the purpose of bringing the appearance of legality to the possession, use and disposal of said monetary funds or other property - shall be punishable by a fine in the amount of up to 120 000 RUB or in the amount of the wage or salary, or any other income of the convicted person for a period of up to one year.
2. The same act committed on a large scale - shall be punishable by a fine in the amount of 100 000 to 300 000 RUB or in the amount of the wage or salary, or any other income of the convicted person for a period of one to two years or by deprivation of liberty for a term of up to four years with or without a fine in the amount of up to 100 000 RUB or in the amount of the wage or salary or other income of the convicted person for a period of up to six months.
3. The act provided for by part two of this article committed: a) by a group of persons in a preliminary conspiracy; b) by a person using his official position - shall be punishable by imprisonment for a term of four to eight years with or without a fine in the amount of up to one million RUB or in the amount of the wage or salary, or any other income of the convicted person for a period of up to five years.
4. The acts stipulated by parts 2 or 3 of this article committed by an organised group - shall be punishable by deprivation of liberty for a term of seven to ten years with or without a fine in the amount of up to one million RUB or in the amount of the wage or salary, or any other income of the convicted person for a period of up to five years.
Note. Large-scale financial transactions and other deals in monetary funds or other property in this article, as well as in article 174.1 of this Code, shall mean financial transactions and other deals in monetary or other property made in an amount exceeding one million RUB.
Articles 174 and 174.1 CC were amended by Federal law no. 162-FZ (8 December 2003) "On introducing amendments and addenda to the Criminal Code ". As a result of this amendment, all ML acts were criminalised irrespective of the amount or value. The Note defines a "large scale" amount, for article 174, item 2 - 4.

- *Acquisition, possession* or *use* is also covered by the elements "acquired by" and "possession and use" in article 174 CC and by article 175 CC dealing with the acquisition of property obtained by crime.

Property that represents the proceeds of crime

94. The money laundering offence extends to any property and monetary funds. The term monetary fund refers to cash and financial deposits, both in any currency. Other property includes all physical objects and property rights (Civil Code, article 128 and 130).

95. It is not necessary to convict a person of a predicate offence to prove that property is the proceeds of crime. The CC does not require this, and law enforcement and the Prosecution Authority have always worked on this basis. This practice has been endorsed by the Supreme Court, which ruled that it is up to the court handing down a sentence for money laundering to establish that property is the proceeds of crime[25].

Predicate offences

96. Russia follows an "all crimes" approach, and 19 of the 20 predicate offences for money laundering required under the FATF Recommendations are covered – offences dealing with insider trading and stock market manipulation are not covered. It should be noted that certain offences, such as fraud, may cover some aspects of these two offences, but that on the whole the offences of insider trading and stock market manipulation are not sufficiently covered. A comparative list of the categories of designated FATF predicate offences that have been covered can be found in Annex 5 of this report. All offences listed in the CC are predicate offences for money laundering, with the exception of 6 offences. Article 174 of the CC stipulates that article 193 CC (non-return from abroad of funds in foreign currency), 194 CC (failure to pay customs payments exacted from an organisation or individual), 198 CC (failure to pay taxes and/or fees from an individual), 199 CC (failure to pay taxes and/or fees from organisations), 199.1 CC (non-fulfilment of tax agent obligations) and 199.2 CC (concealment of funds or property of an organisation or individual business owner, at the expense of which taxes and/or fees must be exacted) are exempted. These excluded offences from the scope of the money laundering offence are penalised through the Criminal Code. However, if charges were instituted under other CC offences, such as fraud, they would fall within the money laundering offence. The offence of possession of property derived from crime in article 175 CC is an element in Russia's money laundering approach. The possession offence covers the possession of any property obtained in a criminal manner. Unlike the offence at article 174 CC, there is no excluded predicate offence for the offence of possession of property derived from crime.

97. Notwithstanding the fact that Russia follows an all crimes approach and that all 19 of the 20 categories of designated FATF predicate offences are covered by the Russian ML offence, the exclusion of the six financial crimes could have a negative effect on the overall effectiveness of the money laundering criminalisation. While the exemptions are generally fiscal in nature it would be possible for defendants to state that the proceeds are the proceeds of one of these crimes. The possibility that a criminal might claim that the proceeds are from one of the exempted offences could discourage law enforcement from pursuing a money laundering investigation for fear of wasting valuable resources on an offence – money laundering – that may not be prosecuted. According to the Russian authorities (section 1.5), the law enforcement community lacks a clear understanding of what (legally) constitutes money laundering. This and the exemption could lead to confusion. Lastly, it will be remembered that according to the Russian authorities (section 1.2), reinvestment into the Russian economy of illegal proceeds taken abroad is one of the main money laundering methods in Russia. That being the case, the exemption of article 193 (non-return from abroad of funds in foreign currency) points to a serious gap in the Russian anti-money laundering regime.

[25] Resolution of the Plenum of the Supreme Court no. 23 (18.11.2004) "On Court Practice on Cases about Illegal Entrepreneurship and Legalisation (Laundering) of Proceeds from Crime" (clause 21).

Extraterritorial predicate offences

98. Jurisdiction to prosecute money laundering extends to predicate offences that occurred outside the territory of Russia. Citizens and permanent residents of Russia who commit a predicate crime outside Russia are subject to criminal liability if the predicate crime that they committed is acknowledged as a crime in the country in which it was committed, and if the offender is not already convicted in the foreign country. Non-residents and stateless persons who commit a predicate crime outside Russia are subject to criminal liability when the crime is directed against the interests of Russia, and in cases stipulated by international agreements, provided they are not convicted in the foreign country and are brought to criminal liability in Russia (CC, article 12).

Self laundering

99. Self-laundering is criminalised in Russia (CC, article 174.1[26]). The article is similar to the regular money laundering offence in article 174.

Ancillary offences

100. Russia's CC includes ancillary and inchoate offences. The table below provides an overview.

Ancillary offences		
FATF terminology	**Article in CC**	**Explanation**
Conspiracy to commit	35	Conspiracy and crime committed by a group where there is agreement on joint commission of the crime
Attempt	30	Preparation and attempts
Aiding and abetting	33(4) and (5)	Aiding and abetting
Facilitating	33(5)	Facilitating
Counselling the commission	33(4) and (5)	Advising and instructing
Other	32	Complicity in a crime

[26] Article 174.1 was translated as follows:
The legalisation (laundering) of monetary funds or other property acquired by the person as a result of a crime committed by him:
1. Making financial operations and other deals in monetary funds or other property acquired by a person as a result of his having committed a crime (except for the offences stipulated by Articles 193, 194, 198, 199, 191.1 and 199.2 of this code) or using these monetary funds or other property for the pursuance of business or other economic activity - shall be punishable by a fine in the amount of up to 120 000 roubles or in the amount of the wage or salary, or any other income of the convicted person for a period of up to one year.
2. The same actions committed on a large scale - shall be punishable by a fine in the amount of 100 000 to 500 000 roubles or in the amount of the wage or salary, or any other income of the convicted person for a term of one to three years or by deprivation of liberty for a term of up to five years with or without a fine in the amount of up to 100 000 roubles or in the amount of the wage or salary, or other income of the convicted person for a term of up to six months.
3. The acts provided for by part two of this article which have been committed: a) by a group of persons in a preliminary conspiracy; b) by a person using his official position - shall be punishable by deprivation of liberty for a term of four to eight years with or without a fine in the amount of up to one million roubles or in the amount of the wage or salary, or any other income of the convicted person for a term of up to five years.
4. The acts stipulated by part 2 or part 3 of this article committed by an organised group - shall be punishable by imprisonment for a term of 10 to 15 years with or without a fine in the amount of up to one million roubles or in the amount of the wage and salary, or any other income of the convicted person, for a period of up to five years.

Additional elements

101. Predicate activity committed outside of Russia by non-resident foreigners or stateless persons, which is not criminalised in the other country, is criminalised in Russia if it concerns a predicate activity that is directed against the interest of Russia or on the basis of an international agreement to which Russia is party.

Recommendation 2

Natural persons that knowingly engage in ML activities

102. According to the legislation only a physical person can incur criminal responsibility, including in those cases when he/she is acting or failing to act in the interests of a legal entity or implementing decisions of the management bodies of that entity. Russian authorities indicate that this principle constitutes one of the fundamental principles of the Russian criminal law. Article 19 of the CC provides that only a sane natural person who has reached the age of 16 years will be subject to criminal responsibility, thus the money laundering and self-laundering offences apply to natural persons that knowingly launder property obtained through the commission of an offence.

Inference from objective factual circumstances

103. Russian prosecutors may rely upon both direct and circumstantial evidence to prove their case in any criminal prosecution. Article 74 of the Code of Criminal Procedure (CCP) provides that knowledge or intent may be proven by direct evidence, or that it may be inferred from the surrounding circumstances, that is, it may be inferred from objective factual circumstances, such as time and place of the crime and motive of the culprit.

Criminal liability for legal persons

104. Under Russian law, legal persons cannot be held criminally liable. There is no provision or statement within the Russian Constitution, nor were the evaluators given any decision from the Supreme Court to the effect that legal persons cannot incur criminal liability. According to the Russian authorities, the fundamental principles of their domestic law as contained in Section 2 of the Russian Constitution, as well as in the Criminal Code and in the Code of Criminal Procedure, moral blameworthiness cannot be extended to legal entities.

105. Russian law, however, provides for corporate and administrative liability for legal persons and a legal person found to have engaged in money laundering activities can have its licence revoked and ultimately be subject to liquidation through civil court proceedings. Furthermore, natural persons operating on behalf of a legal person can be prosecuted.

106. The Russian position concerning legal persons is clear, but is not convincing. It should be noted in this regard that countries party to the European Treaty for Human Rights have applied domestic provisions similar to the Russian provisions concerning freedoms and rights for citizens and the minimum age for natural persons and criminal responsibility. Many countries in Europe also have Constitutional guarantees similar to those found in the Russian Constitution. However, all of these other countries have legislation establishing criminal liability for legal persons.

Sanctions for money laundering

107. There is a wide range of maximum sanctions available for money laundering by natural persons, consisting of increasing fines and terms of imprisonment as the factors surrounding the offence of money laundering become more severe. Fines can be adjusted on the basis of the offender's income. The table below indicates the available sentences for money laundering.

Sanctions for money laundering (natural persons only)		
Crime	**Qualification**	**Punishment**
Money laundering (174 CC)	Ordinary money laundering (RUB 1 million or less)	Fine (max RUB 120 000 or one year annual income)
	Large scale money laundering (more than RUB 1 million)	Fine (RUB 100 000 – 300 000 or one to two years annual income) or Imprisonment (max. four years) and / or fine (max. RUB 100 000 or six months income)
	Large scale money laundering (more than RUB 1 million) & conspiracy or misuse of professional position	Imprisonment (four to 8 years) and / or Fine (max. RUB 1 million or max. five years annual income)
	Large scale money laundering (more than RUB 1 million) or conspiracy or abuse of office as part of an organised group	Imprisonment (7 to 10 years) and / or Fine (max. RUB 1 million or max. five years annual income)
Self laundering (174.1 CC)	Ordinary money laundering (less than RUB 1 million)	Fine (max RUB 120 000 or one year annual income)
	Large scale money laundering (more than RUB 1 million)	Fine (RUB 100 000 – 500 000 or one to three years annual income) or Imprisonment (max. five years) and / or fine (max. RUB 100 000 or six months income)
	Large scale money laundering (more than RUB 1 million) & conspiracy or misuse of professional position	Imprisonment (four to eight years) and / or Fine (max. RUB 1 million or max. five years annual income)
	Large scale money laundering (more than 1 million RUB) as part of an organised group	Imprisonment (ten to 15 years) and / or Fine (max. RUB 1 million or max. five years annual income)

108. The penalty for the offence of preparation regarding money laundering may not exceed half the maximum of the most severe penalty prescribed for money laundering. For the offence of attempting to commit the offence of money laundering, the penalty is three fourths of the maximum penalty of the most severe penalty for money laundering (unfinished crime, article 66 CC). According to article 34 of the CC (part 3) the criminal responsibility of an instigator and accessory shall ensue under the article providing for punishment for the crime committed, with reference to article 33 of the CC providing for the types of accomplices of the crime. Thus they bear responsibility equally with executors of the crime under the relevant part of article 174 of the CC:

109. The degree of responsibility depends on the specific participation in the crime. As a rule, it is somewhat lower than in the case of the person committing the crime. These people would be subject to sanctions under the same article of the CC as the person who committed the crime, that is, the verdict defines their role in committing the crime with reference to article 33 of the CC.

110. Punishment for the conspiracy to launder proceeds is imprisonment for a term of four to eight years with or without a fine in the amount of one million roubles or in the amount of the wage or any other income of the convicted person for a period of up to five years

Statistics

111. Russia provided the evaluation team with statistics related to *i)* the number of ML crimes investigated, *ii)* the number of persons investigated for money laundering, *iii)* the number of completed money laundering investigations, *iv)* the number of persons charged with money laundering, *v)* the number of money laundering cases sent to court, and *vi)* the number of convictions related to money laundering. All these statistics can be found in the tables below. The first table with statistics on convictions related to money laundering includes convictions for other (more) serious crimes for which money laundering or self laundering was only considered an aggravating crime. The last two tables also contain statistics on convictions, but these numbers represent stand alone convictions.

Money laundering: investigations 2003 – 2006				
	Year	**Money laundering**	**Self laundering**	**Total**
Number of ML crimes investigated	2003	481	137	618
	2004	271	1 706	1 977
	2005	524	6 937	7 461
	2006	631	7 326	7 957
	Total	**1 907**	**16 106**	**18 013**
Number of persons investigated for money laundering	2003	126	55	181
	2004	118	577	695
	2005	261	2 227	2 488
	2006	205	2 417	2 622
	Total	**710**	**5 276**	**5 986**
Number of completed money laundering investigations	2003	471	112	583
	2004	222	1 549	1 771
	2005	377	6 359	6 736
	2006	582	6 942	7 524
	Total	**1 652**	**14 962**	**16 615**
Number of persons charged with money laundering	2003	68	49	117
	2004	93	552	645
	2005	232	2101	2 333
	2006	146	2170	2 316
	Total	**539**	**4 872**	**5 411**

Money laundering: prosecutions 2003 – 2006				
	Year	**Money laundering**	**Self laundering**	**Total**
Number of money laundering cases sent to court	2003	364	101	465
	2004	145	1 490	1 635
	2005	305	6 079	6 384
	2006	452	6 428	6 880
	Total	**1 266**	**14 098**	**15 364**

Money laundering as an aggravating offence: convictions 2003 – 2006				
	Year	**Money laundering**	**Self laundering**	**Total**
Number of convictions related to money laundering (includes convictions for more or other serious crimes for which money laundering or self laundering was only considered an aggravating crime).	2003	11	3	14
	2004	14	42	56
	2005	126	293	419
	2006	109	423	532
	Total	**260**	**761**	**1 021**

Money laundering: stand alone convictions 2003 – 2006					
Year	**2003**	**2004**	**2005**	**2006**	**Total**
Imprisonment	-	1	5	9	15
Conditional imprisonment	3	2	7	5	17
Fine	-	-	7	11	18
Total Sanctions	**3**	**3**	**19**	**25**	**50**

Self-laundering: stand alone convictions 2003 – 2006					
Year	**2003**	**2004**	**2005**	**2006**	**Total**
Imprisonment	-	5	14	32	51
Conditional imprisonment	-	7	14	47	68
Fine	-	-	12	14	26
Total Sanctions	**0**	**12**	**40**	**93**	**145**

Effectiveness of the money laundering provisions

112. Russia is largely compliant with the FATF requirements dealing with criminalisation of ML. Russia has progressively improved its effectiveness in implementing the ML offence. The ML offences are being used increasingly, with ML investigations jumping from 618 in 2003 to 7 957 in 2006 and with the number of money laundering cases sent to court going from 465 in 2003 to 6 880 in 2006. In a country where, based on the information available, corruption is a significant problem, including corruption in the police and the judiciary, and where there is an acknowledged problem with organised crime, there should be higher numbers for both the number of ML cases being investigated and cases going to court. Moreover, the overall number of convictions is somewhat low (from 14 in 2003 to 532 in 2006). Accordingly, Russia should continue to make progress in the use of its ML offence.

2.1.2. Recommendations and Comments

113. Russia should establish offences of insider trading and stock market manipulation.

114. Russian authorities should reconsider their position concerning the criminal liability of legal persons in light of the position taken by several European countries with similar constitutional and fundamental principals in their domestic law as those found in Russia.

2.1.3 Compliance with Recommendations 1 & 2

	Rating	Summary of factors underlying rating
R.1	**LC**	• Russia has not established offences of insider trading and stock market manipulation.
R.2	**LC**	• Russia has not established criminal liability for legal persons.

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and Analysis

Criminalisation of terrorist financing

115. Russia ratified the UN Convention for the Suppression of the Financing of Terrorism of 1999 in July 2002. As part of the ratification act, Russia criminalised terrorist financing in article 205.1 CC[27]. The article targets any support or contribution to terrorist activity, and financing of terrorism is explicitly mentioned in the first part of the article. Financing of terrorism is additionally defined and explained in note 1 to this article. The language of Note 1 is in line with the definition of financing of terrorism in article 3 of the AML/CFT Law.

116. Russia's criminalisation of TF is consistent with the 1999 UN Convention for the Suppression of the Financing of Terrorism. It is also in line with UN Security Council Resolution 1373. Note 1 of Article 205.1 refers to "funds" and "financial services". The term "funds" is not defined in this note. However, Presidential Decree No. 6 of 28.9.2001 on UNSCR 1373 uses the same language as that used in UNSCR 1373 and mentions that the measures to be taken against terrorist property applies to funds, financial assets and economic resources. It should be noted, as has been noted earlier in the Report (in Section 1.1) that the Russian Constitution, at Article 15, provides that norms from international agreements once ratified by Russia become a component of the Russian legal system. Accordingly, the definition of 'funds' as defined in the UN Convention for the Suppression of Terrorist Financing is applicable in Russian law.

117. The criminalisation also covers the provision and collection ("raising") of funds. The financing of terrorism is connected to 10 crimes of terrorist nature[28], committed by both individual terrorists and terrorist organisations. However, it does not extend to the theft of nuclear material as

[27] Article 205.1 CC (Contributing to Terrorist Activity) was translated as follows:
1. The soliciting, recruiting or other inveiglement of a person for committing any of the crimes envisaged by Articles 205, 206, 208, 211, 277, 278, 279 and 360 of the present Code, the arming or training of a person for the purpose of committing any of the said crimes, and equally the financing of terrorism - is punishable by a term of imprisonment of four to eight years.
2. The same acts committed by a person through the abuse of his/her office - are punishable by a term of imprisonment from seven to fifteen years either with a fine in an amount of up to one million roubles or in the amount of the convict's wage or another income for up to five years or without such a fine.
Note 1: In the present Code "the financing of terrorism" means the provision or raising of funds or the provision of financial services in the knowledge of their being intended for financing the organising, preparing or committing at least one of the crimes envisaged by Articles 205, 205.1, 205.2, 206, 208, 211, 277, 278, 279 and 360 of the present Code or for supporting an organised group, illegal armed formation, criminal community (criminal organisation) formed or being formed to commit any of the said crimes. Note 2: A person that has committed a crime set out in the present article shall be relieved from criminal liability if by a timely notice to authorities or otherwise the person has assisted in the prevention or stopping the crime financed and/or contributed to by the person, unless the person's actions contain another corpus delicti.

[28] The 10 acts are: articles 205 (terrorist act), 205.1 (contributing to terrorist activity), 205.2 (public calls for committing terrorist activity or public justification of terrorism), 206 (hostage-taking), 208 (organisation of an illegal armed formation or participation in it), 211 (hijacking an aircraft or a ship or a railway train), 277 (encroachment on the life of a statesman or a public figure), 278 (forcible seizure of power or forcible retention of power), 279 (armed rebellion) and 360 (assaults on persons or institutions enjoying international protection).

required under the UN Convention for the Suppression of the Financing of Terrorism. The legislation requires that the provision or collection of funding be connected to the financing of the commission of a terrorist act or that it be intended to finance the preparation of a terrorist act.

118. Intent is required, but the Prosecution Authority does not need to prove that the funds are intended or had been intended to finance a specific terrorist act. Terrorist financing is committed as soon as the funds are collected, regardless of whether or not the funds are used in the commission of a terrorist act.

119. The definition of terrorist financing also includes the provision of financial services, although that term is not further defined in the law. Preparation to commit terrorist financing is also covered (unfinished crime). Terrorist financing is a predicate offence for money laundering. Article 205.1 provides a defence for the person who has committed a terrorist financing offence and, in a timely manner, assists in the prevention of the crime that is being financed.

Terrorist Financing as a predicate offence for ML

120. The offence of terrorist financing is a predicate offence caught by the "all offences" approach used for the money laundering offence in the CC. The Code's provisions dealing with inchoate and ancillary offences apply to the TF offence.

Jurisdiction over TF offences

121. Terrorist financing can be punished regardless of the location of the person alleged to have committed the crime and the location of the terrorist or terrorist organisation or the location where the terrorist act is (will be) committed if the act is committed by citizens of Russia or by stateless persons permanently residing in Russia. If the crime is committed by foreign citizens or by stateless persons who do not permanently reside in Russia, terrorist financing can only be punished if the act is considered to be directed against the interests of Russia, its citizens and non-citizen residents, or if the act can be punished based on specific provisions in international agreements signed by Russia.

Inference from objective factual circumstances and criminal liability for legal persons

122. As with money laundering, the TF provision applies to natural persons that knowingly finance terrorism. The law also permits the intentional element of the TF offence to be inferred from objective factual circumstances. As is the case for money laundering, legal persons do not face criminal liability. According to the Federal law "On combating terrorism", however, legal persons can incur administrative and civil responsibility for financing or for providing any other support of terrorism.

Sanctions

123. The punishment for TF is 4 to 8 years imprisonment. If the same crime is committed by a person through the abuse of his office, the punishment is 7 to 15 years imprisonment. In this last case, the judge may add a fine to the prison sentence (max. RUB 1 million or maximum five years annual income). The penalty for a legal person is in the form of liquidation by a court ruling with confiscation of all their property for the benefit of the state.

124. The penalty for the offence of preparation regarding TF may not exceed half the maximum of the most severe penalty prescribed for TF. For the offence of attempting to commit the offence of TF, the penalty is three-fourths of the maximum penalty of the most severe penalty for TF (unfinished crime, article 66 CC). According to article 34 of the CC (part 3) the criminal responsibility of the instigator and accomplice is applied under the article stipulating the sanction for committing the crime, *i.e.* they bear responsibility equally with those who commit the crime.

125. The degree of responsibility depends on the specific participation in the crime. As a rule, it is somewhat lower than in the case of the person committing the crime. These offenders bear sanctions under the same article of the CC as the offender who committed the crime (under article 205.1 of the CC), at this the verdict defines their role in committing the crime with reference to article 33 CC.

Statistics

126. Russia provided the evaluation team with statistics related to *i)* the number of TF crimes investigated, *ii)* the number of persons investigated for TF, *iii)* the number of completed TF investigations, *iv)* the number of TF cases sent to court, and *v)* the number of persons convicted of TF. All these statistics can be found in the tables below.

Terrorist financing: investigations 2003 - 2006		
	Year	**Number**
Number of TF crimes investigated	2003	No statistics available
	2004	16
	2005	4
	2006	15
	Total	**35**
Number of persons investigated for TF	2003	No statistics available
	2004	4
	2005	18
	2006	21
	Total	**43**
Number of completed TF investigations	2003	No statistics available
	2004	3
	2005	12
	2006	9
	Total	**24**

Terrorist financing: prosecutions 2003 - 2006		
	Year	**Number**
Number of TF cases sent to court	2003	No statistics available
	2004	2
	2005	14
	2006	9
	Total	**25**

Terrorist financing: convictions 2003 - 2006		
	Year	**Number**
Number of persons convicted of TF	2003	No statistics available
	2004	2
	2005	15
	2006	7
	Total	**24**

Effectiveness of the terrorist financing provision

127. The Russian provisions dealing with TF offences are largely compliant with the FATF requirements. The TF offences have been used with 24 persons being convicted in 2004 – 2006. Among the 24 persons convicted in 2004 – 2006 under article 205.1 of the CC, all were sentenced to deprivation of liberty for the term of four to 15 years (in average about eight years to each of them). Russia has, over the past several years, had significant exposure to terrorist activities. Given this level of terrorist activity, the low number of cases and convictions suggests that the Russian terrorist financing provision could be used more effectively.

2.2.2 Recommendations and Comments

128. The TF offence criminalises the financing of offences that are listed in the annex to the *Terrorist Financing Convention* with the exception of the theft of nuclear material. Russia should establish this offence and expand the TF offence to include this new offence.

129. Russian authorities should reconsider their position concerning the criminal liability of legal persons in light of the position taken by several European countries with similar constitutional and fundamental principals in their domestic law as those found in Russia.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**LC**	• The terrorist financing offence does not extend to the theft of nuclear material, as required in the UN Convention for the Suppression of the Financing of Terrorism. • Russia has not established criminal liability for legal persons.

2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)

2.3.1 Description and Analysis

General

130. Russia possesses a dual procedure for dealing with confiscation. The CC and CCP both contain provisions that authorise the confiscation of proceeds of crime while the CCP contains provisions to forfeit "instrumentalities."

Confiscation of proceeds

Criminal Code

131. The confiscation of proceeds of crime is covered by article 104.1 CC. This provision came into being in July 2006 and came into force in 2007. The approach taken prior to the new provision was that contained in article 81 of the Code of Criminal Procedure (see section on Confiscation of Instrumentalities below). The new legislation was introduced in part because it was considered by some to be inappropriate to use the Code of Criminal Procedure to confiscate proceeds. The new approach taken is based on a list of Criminal Code offences to which article 104.1 CC applies. The list includes most serious crimes but does not include the offences relating to money laundering. An application must be made to the court by the appropriate authority in order to obtain a confiscation.

132. Article 104.1 CC allows for the confiscation of property that is derived directly or indirectly from the proceeds of crime, including income and property resulting from proceeds that have been transformed. This provision can also be used to confiscate proceeds that have been co-mingled with legitimate property. Article 104.1 CC can also be used to confiscate proceeds that have been

transferred to another person if that person knew or should have known that the property was obtained through the commission of an offence.

133. Article 104.2 CC permits a court to issue an order confiscating an amount of money corresponding to the value of proceeds that have been dissipated or are otherwise no longer available for confiscation.

Code of Criminal Procedure

134. Article 81 CCP permits the procedural confiscation of proceeds that are derived directly or indirectly from the commission of an offence, including income and property resulting from proceeds that have been transformed. This provision can also be used to confiscate proceeds that have been co-mingled with legitimate property. This provision was used extensively prior to the coming into force of the new confiscation legislation (see section on Statistics below). Unlike article 104.1 CC, article 81 CCP is not restricted to a list of criminal offences and can be used to obtain the confiscation of proceeds from any offence, including the proceeds from the money laundering offences.

Confiscation of instrumentalities

135. Both article 104.1 CC and article 81 CCP allow for the confiscation of instruments, equipment or other means of committing an offence or intended to be used to commit a crime. Property used or intended to be used for financing terrorism, an organised group, an illegal armed formation or a criminal organisation can be confiscated pursuant to article 104.1 part 1 (c) CC.

Scope of property

136. The Russian confiscation regime does not make any distinction between money, valuables or any other property; all of these are treated in the same way in the Criminal Code and the Code of Criminal Procedure.

Provisional measures

137. Seizure of property and freezing of accounts in criminal cases is governed by the Code of Criminal Procedure (articles 81, 115, 116 and 165). Seizure can be executed against both proceeds of crime and instruments. Seizures are executed against property in order to ensure future enforcement of judgements or to gather evidence. Seizure is only allowed if approved by a judge. Any investigator, with the consent of the head of investigative body, and any inquirer with the consent of the prosecutor, can file a petition at a district court and request a court order to seize and freeze property. In urgent cases, an investigator may act without prior order, but the courts must be notified of any action within 24 hours. Should the court deem that a seizure has taken place illegally, the seized property will be returned. Money in bank accounts can also be seized; this takes place by freezing all transactions on an account.

138. Seizure applications are dealt with on an *ex parte* basis.

Powers to identify and trace property

139. Articles 165 and 182 to 186 CCP allow competent authorities to seize documents from financial and other relevant institutions and from individuals, thus permitting them to identify and trace property that is or may become the subject of confiscation.

Protection of bona fide third parties

140. *Bone fide* third party rights are protected by article 123 of the Code of Criminal Procedure. This article gives the right to a person whose interests have been infringed by any act or decision of a body of inquiry, of an inquirer, an investigator, a prosecutor or of a court to appeal that act or decision.

Authority to void actions and contracts

141. Article 169 Civil Code provides that any transaction contrary to the fundamentals of law and order or to morality is void. The courts have the legal authority pursuant to article 169 CC to declare that a transaction or contract is void. This provision has been used by a Russian lower court to void a transaction and the decision was subsequently endorsed by the Russian Supreme Court.

Additional elements

142. Pursuant to article 243 of the Civil Code property can be forfeited civilly by a court as a sanction for commission of a crime or any other offence.

Statistics

143. In 2005 and 2006, Russia seized or froze property in 491 ML incidents, comprising 15 418 cases. Confiscation in ML cases between 2003 and 2006 amounted to over RUB 680 million (with over RUB 385 million in 2006 alone), which averages out to RUB 170 million per year in all ML and self laundering cases.

144. Russia also keeps statistics on the amounts frozen/seized and confiscated between 2003 and 2006 for predicate offences. Freezing/seizure totalled an amount of RUB 52.5 billion (an average of about RUB 13 billion per year) for the years 2003-2006, while confiscation in respect of all crimes for the same period totalled RUB 75.5 billion (an average of about RUB 19 billion per year).

Statistics for confiscation and freezing				
Money laundering only				
	Years	**Total**	**Article 174 CC**	**Article 174.1 CC**
Number of cases of freezing or seizure of property	2003	No data		
	2004	No data		
	2005	264	53	211
	2006	227	16	211
	Total	**491**	**69**	**422**
Amounts frozen or seized (x 1000 RUB)	2003	185 880	75 207	110 673
	2004	62 506	4 806	57 700
	2005	739 707	32 312	707 395
	2006	563 071	80 621	482 450
	Total	**1 551 164**	**192 946**	**1 358 218**
Amounts confiscated (x 1000 RUB)	2003	112 079	13 883	98 196
	2004	103 191	4 388	98 803
	2005	79 174	13 139	66 035
	2006	385 992	36 474	349 518
	Total	**680 436**	**67 884**	**612 552**

Statistic for seizure, confiscation and freezing		
All criminal cases		
	Years	**Amount**
Amounts on freezing/seizure in criminal cases (x 1000 RUB)	2003	4 941 612
	2004	8 187 820
	2005	19 617 689
	2006	19 901 258
	Total	**52 648 379**
Confiscated amounts in criminal cases (x 1000 RUB)	2003	5 905 368
	2004	37 221 468
	2005	16 903 737
	2006	15 516 942
	Total	**75 547 515**

2.3.2 Recommendations and Comments

145. With two procedures for dealing with confiscation, Russia's system of confiscation appears complex, but in effect they are complementary. The procedural confiscation that is available in the Code of Criminal Procedure may be vulnerable to criticism by the courts and others. Russia should consider expanding the confiscation provisions in its Criminal Code to include at the very least the money laundering offence. There is no policy reason as to why confiscation should not apply to all offences that are committed for a profit motive. In this regard, evaluators were informed that consideration is being given to the expansion of the Criminal Code provisions dealing with confiscation.

146. The new confiscation regime (CC articles 104.1 – 104.3) has only been in effect since 1 January 2007 and so it is difficult to evaluate its effectiveness. Russian authorities have made good use of the old provision under article 81 of the Code of Criminal Procedure as evidenced by the value of confiscation for the ML offences at over RUB 385 million in 2006 and total confiscations for all crimes valued at over RUB 75 billion between 2003 and 2006. The new provisions should be less vulnerable to criticism and therefore should be more effective in targeting proceeds of crime.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	**C**	• This Recommendation is fully observed.

2.4 Freezing of funds used for terrorist financing (SR.III)

2.4.1 Description and Analysis

General description and legal basis

147. Russia has implemented the United Nations Security Council Resolutions (UNSCRs) concerning combating terrorism financing through Presidential Decrees: Decree 786 of 5 May 2000 (targets UNSCR 1267); Decree 266 of 6 March 2001 (targets UNSCR 1333); Decree 6 of 10 January 2001 (targets UNSCR 1373); and Decree 393 of 17 April 2002 (targets UNSCR 1390).

148. In this context, the Presidential Decrees have the force of federal law on the basis of a ruling of the Constitutional Court[29] which recognised the right of the President, in the absence of regulations by law on a given issue, to execute such regulations autonomously. These Decrees oblige all bodies of state power, state institutions and organisations of Russia, as well as all Russian commercial and non-profit entities, legal and physical persons under the jurisdiction of Russia to take measures to freeze respective assets of terrorists. According to the Decrees, all assets of terrorists and terrorist organisations listed in the UNSCR, as well as all assets belonging to persons and organisations owned or controlled by them, are frozen without time limitation or until there is a de-listing by the UN.

149. The UNSCRs are also implemented through the mechanism envisaged in the AML/CFT Law and Ordinance of the Government No. 27 of 18 January 2003 (Terrorist Financing Regulation). This mechanism consists of a listing process which is explained below. Taken together, these decrees, the law and the ordinance allow the Russian government to freeze terrorist assets.

150. The actual freezing of terrorist property results from entities being listed by Russian authorities, and the freezing is made operational by financial institutions and others. Once an entity is listed, institutions are no longer permitted to perform transactions involving funds or assets (effectively freezing) owned or controlled by the listed entity.

Obligations implemented under UNSCR 1267 (and successor resolutions) and UNSCR 1373

151. The Presidential Decrees for implementation of the UNSCRs, the AML/CFT Law and the Terrorist Financing Regulation[30] together provide for the essential elements of the legal framework for freezing terrorist property pursuant to the obligations contained in UNSCRs 1267 and 1373.

152. The AML/CFT Law and the Terrorist Financing Regulation contain the rules for drawing up a terrorist list. This list consists of two parts. The first part consists of all persons designated under UNSCR 1267 (and successor resolutions), as well as persons included in other lists compiled by international organisations combating terrorism, and by the bodies authorized by them and recognised by Russia. This part is also referred to as the "international list".

153. The second part is called the "national list". The national list includes the names of entities that are identified and designated by the Russian authorities in accordance with the AML/CFT Law and the Terrorist Financing Regulation.

154. With respect to the international list, the Presidential Decrees provide the basis for permanently blocking the assets of persons and organisations identified in the UNSCRs and subsequently listed by the Russian authorities. The AML/CFT Law creates an obligation on financial institutions performing transactions in respect of suspected funds and other assets immediately to freeze (without a court decision) all transactions involving these funds or other assets, if at least one of the parties in the transaction is a listed entity or is an entity that is directly or indirectly owned or controlled by the listed entity or is acting on behalf of or on the instruction of such a listed entity.

155. The complete list is assembled on the basis of data submitted by the General Prosecutor's Office, ROSREG, the MoJ and the MFA.

156. The AML/CFT Law indicates the possible legal grounds for designating an entity. For example, an entity will be listed if:

- A court decision of Russia has entered into legal force regarding the liquidation or banning of an organisation because of its involvement in extremist activities or terrorism.

[29] No. 11-P of 30.04.1996.

[30] Government Ordinance no. 27 of 18.01.2003 "On approval of Regulations on identification of the list of organisations and individuals in relation to whom there is information about their participation in extremist (terrorist) activities".

- A conviction has entered into legal force regarding a natural person found guilty of committing a terrorist crime.
- There is an order of an investigator to initiate either a criminal case against a person who has committed a terrorist crime or proceedings against an organisation.
- An entity appears on a list compiled by international organisations combating terrorism, or by bodies authorised by them, of organisations and persons linked to terrorist organisations or terrorists, and recognised by Russia.

157. The list is disseminated to all financial institutions, financial supervisory bodies, DNFBPs and regional offices of Rosfinmonitoring for their consideration and action in accordance with the AML/CFT Law.

158. The effect of being listed consists of a temporary suspension of financial operations (freezing) in respect of all assets owned or controlled by the listed entity. The freezing is reported to Rosfinmonitoring. This suspension is in effect for an initial two working days, during which time Russian authorities verify the basis for the freezing action. The freeze can be extended for an additional five working days if required in order to complete the verification.

159. In the case of an entity listed on the international part of the list, the freeze is permanent or until the UN or other international organisation de-lists it. In the case of an entity on the national list, the freezing is lifted after verification as to whether there were insufficient grounds to freeze the assets, or the case is turned over to law enforcement for further investigation and prosecution, in which case the authorities will seize the assets in their own right. The seizure will remain in effect until the completion of the case.

160. The complete list is compiled by Rosfinmonitoring and is updated regularly. As of 28 June 2007, Rosfinmonitoring had published the 18th edition of the list. This edition contained in total 2 464 persons, with the international list containing 489 entities (364 natural and 125 legal persons), and the national list containing 1 975 persons (1 950 natural and 25 legal persons). The list is also updated immediately after the 1267 Sanctions Committee list is updated.

161. It should be noted that the entire list is not published. The list is available on the Rosfinmonitoring secure web-site and the names of organisations that are listed on the national list are published in the Russian Gazette, and, of course, the list is distributed to all the relevant financial institution and DNFBPs. The list is not available to the general public.

Freezing of funds

162. If a financial institution ("an organisation that carries out operations with monetary funds or other assets") detects a transaction by a designated entity or by a designated entity owned or controlled by a designated entity, the transaction is reported to Rosfinmonitoring and suspended (frozen) for two days. This suspension is performed without prior notice to the listed customers and other persons (article 4 and 7, AML/CFT Law). Funds transferred from outside of Russia to a listed entity can occur, however, these transactions are reported to Rosfinmonitoring and these funds will be frozen. If, after the two day period the financial institution does not receive a further order directing the continued suspension of the transaction from Rosfinmonitoring, the financial institution will perform the transaction according to the customer's request.

163. Assessors were informed that no funds were frozen in respect of entities listed pursuant to UNSCR 1267. However, a UN Report[31] suggests that Russia confiscated property in relation to Resolution 1267. Russian authorities have explained that the information provided to the UN through

[31] "Third report of the Analytical Support and Sanctions Monitoring Team Appointed Pursuant to Resolution 1526 (2004) concerning Al-Qaida and the Taliban and Associated Individuals and Entities".

their ambassador at the UN was misinterpreted and have confirmed that, in effect, no funds have been frozen in respect of UNSCR 1267.

164. Once Rosfinmonitoring receives the report of a frozen transaction, it will perform a preliminary check to assess the reasonableness of the suspension of the operation. If the suspension of the transaction undertaken by the reporting institution is considered justified, Rosfinmonitoring will issue an order requesting a further suspension of the transaction for a term of up to five days and send it to the reporting institution, as well as refer the relevant information for operative action to law enforcement bodies (AML/CFT Law, article 8).

165. The law enforcement bodies will start operative actions and investigate all information on the suspended transaction sent by Rosfinmonitoring, will inform Rosfinmonitoring about the results and will take a decision on further procedural actions (seizure) in relation to the assets recognized as belonging to a terrorist. Until the end of the investigation by the law enforcement bodies, the blocked funds will remain frozen. If necessary, the investigator conducting the investigation has the right to seize the frozen assets before the seven days run out even before the investigation is finished, on the basis of the provisions of art. 115 of the Code of Criminal Procedure.

166. All reports containing information suggesting that an offence has been committed are checked by law enforcement bodies as required by articles 144 and 145 CCP.

Definition of funds

167. Presidential Decree No. 6 of 10.01.2002 on UNSCR 1373 uses the same language as that used in the UNSCR and mentions that the measures to be taken against terrorist property apply to funds, financial assets and economic resources. The measures apply to all funds and economic resources of persons committing or attempting to commit terrorist acts or who participate in the commission of terrorist acts or render support to their commission; of organisations owned or controlled, directly or indirectly by such persons as well as persons or entities acting on behalf of or at the direction of such persons and entities including the funds received or acquired through property directly or indirectly owned or controlled by such persons, and related to these persons and entities.

Examining and giving effect to freezing mechanisms of other jurisdictions

168. There is no effective law and procedure in place to examine and, if appropriate, give effect to, freezing orders of other jurisdictions. If informed by a foreign FIU that a freezing action has occurred in the foreign state, Rosfinmonitoring will monitor the activities of the target entity in Russia. Russian authorities are able to give effect to designations under freezing mechanisms of other jurisdictions but it is by way of a mutual legal assistance request or by way of an existing MOU or agreement signed with another country. No MOU or agreement has been signed to date. Using the MLA approach does not ensure that prompt action can be taken.

169. Of course, asset freezing action in another jurisdiction may also give Russian law enforcement agencies information suggesting that an offence under their law may have been committed. The relevant Russian law enforcement agencies may investigate such an offence and during such an investigation may seize assets with subsequent confiscation within a court procedure.

System for communicating actions to the financial sector

170. Rosfinmonitoring maintains a comprehensive list of all listed persons subject to asset freezing. This list (its international and national parts) is updated when changes are made to add, amend or delete information concerning listed entities. The amendments are introduced into the appropriate part of the List depending on whether that change is made by the UN or Russia. The terrorist list is distributed electronically or on paper within one day of any change made to it to all

financial institutions. It is also available on the secure website of Rosfinmonitoring, to which financial institutions, supervisory authorities and DNFBP's have access.

171. Russian authorities do not communicate freezing actions taken by financial institutions to other financial institutions. However, Russian authorities engage in indirect feedback by way of holding seminars and workshops for financial institutions where money laundering and terrorist financing typologies are discussed. Moreover, Russian authorities provide a measure of general feed-back information to banks through the Russian Banking Association.

Guidance to financial institutions and DNFPBs

172. Guidance is provided by supervisory bodies to the institutions for which they are responsible. The BoR provides guidance to all credit institutions and Rosfinmonitoring provides guidance to all financial institutions and designated non-financial businesses and professions not falling within the responsibilities of other supervisory authorities. The guidance covers the relevant provisions of the AML/CFT Law, informs the institutions of the existence of the terrorist lists and explains the procedure for working with the lists and the procedure for suspending financial transactions. The guidance contains information for the development and implementation of internal control rules, and deals with having to submit reports in a timely fashion to the reporting entities

Publicly-known procedures for considering de-listing requests and for unfreezing the funds of de-listed persons

173. As described above, the Russian authorities have established a list comprised of two sections – an international list and a national list.

174. It should be noted at the outset that requests for unfreezing funds cannot occur for the first seven days that funds have been frozen by a financial institution since the subject of the freezing action will not have been made aware or informed of the freezing action. If, however, during the first seven days a case is turned over to law enforcement, then the procedure for delisting and unfreezing in respect of entities listed on the national list and described below would apply.

175. With respect to the international list, Russian authorities will forward a request to be de-listed or to have funds unfrozen, to the UN Committee dealing with Resolution 1267 and will then abide by whatever decisions the Committee reaches. This procedure taken by Russia is not publicly known.

176. With respect to the national list, there is no special procedure provided. De-listing and unfreezing of funds can be made by applying to the courts for the appropriate action as per the provisions of the Code of Criminal Procedure.

177. The Russian authorities have indicated that all entities who are listed are either being investigated, on trial or have been convicted for terrorist activities. The list does not contain any entity that is suspected of committing a terrorist offence. The Russian authorities contend, therefore, that in all of these situations, the entity will either be aware that it has been listed or the lawyer representing the entity will know of the listing and will so inform the entity he represents. This approach is based on a number of assumptions, such as the entity or its representative is aware that it is listed or that it or its representative is aware of the procedure to be de-listed. Such assumptions are difficult to sustain.

Publicly-known procedures for unfreezing the funds or other assets of persons or entities inadvertently affected by a freezing mechanism

178. Entities listed on the Russian national list are the names of entities that have been convicted, are at trial or are being investigated. Under the circumstances, the Russian authorities indicated that it is impossible for someone to have been listed by inadvertence. In the case of a listed entity that is

being tried and ultimately acquitted, the name of the entity is removed from the list and the funds are unfrozen. For the entity being investigated, the funds are unfrozen if the investigation is terminated without going to trial.

Authorising access to funds for certain basic expenses in accordance with UNSCR 1452

179. Russian authorities have not frozen any funds or other assets pursuant to UNSCR 1267 and therefore have no experience in authorizing access to funds for basic expenses in accordance with UNSCR 1452.

180. However, if a request to access funds for basic needs were to arise, Russians officials informed the assessors that a request could be submitted to Rosfinmonitoring or to a court for a decision concerning the request. Russian officials would then submit the request to the UN Committee on Resolution 1267 for comment.

Right to challenge freezing measures

181. An entity listed on the national list has the possibility to challenge the freezing of the funds in court. From a practical perspective challenging the freezing measure is not likely within the initial freezing period because the entity will be unaware of the measure taken against it. After the initial freezing period, the measure is either lifted or the case is turned over to law enforcement. Where the case is turned over to law enforcement for further investigation, the entity can challenge the measure through the normal court process as provided for in the Code of Criminal Procedure.

Freezing, seizing and confiscation in other circumstances

182. Russian law enforcement authorities may apply certain other measures in the context of a criminal investigation or prosecution to seize or confiscate assets suspected or proven to be related to terrorist financing. These measures include:

- A court can order the seizure of property in connection with the investigation related to terrorist offences (including financing of terrorism). This property may be confiscated upon conviction for these offences.
- The court may also seize property or place it under restraint or freezing order pursuant to a request for mutual legal assistance.

Protecting bona fide third parties

183. There are no special provisions dealing with the protection for bona fide third parties. Russian authorities indicate that article 123 of the Code of Criminal Procedure is the main source of protection for third party rights. This provision allows for, inter alia, a person whose interests may have been impacted by actions or decisions taken by an investigator, prosecutor or a court to seek assistance by way of an appeal to the court.

184. As mentioned above, property frozen because it belongs to or is controlled by a terrorist that is listed on the national terrorist list can be turned over to investigators. At this point the normal criminal process is engaged. From this point onward, article 123 would apply and bona fide third parties can seek to have their interests protected through the courts.

185. In the case of an entity listed on the international list, article 22 of the Russian Code of Civil Procedure allows a person to apply to the courts in order to resolve any disputes over claims concerning the right to funds or other assets.

186. From a practical perspective, no protection is afforded in the initial two-seven days of a freezing because neither the listed entity nor an innocent third party would be aware that their property has been frozen.

Monitoring compliance with freezing obligations

187. Rosfinmonitoring supervises the execution of freezing measures by financial institutions not supervised by a supervisory body. The BoR and other supervisory bodies monitor other financial institutions for which they are responsible. If a financial institution is discovered not to comply with the freezing obligations, there are sanctions for non-compliance contained in the AML/CFT Law and the Code on Administrative Offences. Those sanctions apply to all designated financial institutions and DNFBPs. The main punishment is the withdrawal of the licence of the business that is in non-compliance and the imposition of fines.

188. In the case of non-financial institutions and of physical persons, no monitoring occurs. However, the obligation to freeze funds and other assets belonging to terrorists applies to them as well as to financial institutions and if a failure to freeze such property is discovered, the appropriate penalties, either administrative or criminal, will apply.

Additional elements

189. Certain types of financial operations of listed entities are not suspended by Rosfinmonitoring. These include payment for certain types of expenses and services, payment for household expenses etc. Credit institutions must mention the purpose of the payment for each specific operation.

Statistics

190. The table provides an overview of the number of suspended transactions and the amounts frozen.

Suspended transactions and amounts frozen		
	Year	**Number**
Number of suspended transactions (national terrorist list only)	2003	0
	2004	4
	2005	8
	2006	7
	Total	**19**
Amounts frozen (USD) (national terrorist list only)	2003	0
	2004	5 988
	2005	489 054
	2006	28 438
	Total	**523 480**

2.4.2 Recommendations and Comments

191. Russia implements UNSCRs 1267 and 1373 through the implementation of Presidential Decrees on UNSC Resolutions 1267, 1333, 1373 and 1390 and the application of the AML/CFT Federal Law and the Government Decision on the Financing of Terrorism. These instruments are made operational through the drafting of a list containing the names of entities whose funds and assets must be frozen by all financial institutions, DNFBPs and others.

192. While the freezing mechanisms are in line with the UN Resolutions, there are elements associated with Special Recommendation III that are either absent or are incomplete in the Russian approach. In implementing UNSCR 1373, Russia relies heavily on the criminal justice system for covering the various elements contained in SRIII. Reliance on the criminal justice system risks creating problems regarding the efficient implementation of this Resolution. For example, difficulties in obtaining sufficient evidence to convict may result in a terrorist being acquitted and his funds unfrozen. Such a result would frustrate the objectives of UNSCR 1373.

193. Russia needs to implement a national mechanism to examine and give effect to actions initiated under the freezing mechanisms of other jurisdictions.

194. Russia should establish an effective and publicly known procedure for dealing with de-listing requests and for dealing with requests to unfreeze in a timely manner the funds or other assets of entities that have been inadvertently affected by a freezing action.

2.4.3 Compliance with Special Recommendation III

	Rating	Summary of factors underlying rating
SR.III	**PC**	• Reliance on the criminal justice system risks creating problems with the effective implementation of UNSCR 1373. • Russia does not have a national mechanism to examine and give effect to freezing actions taken by other countries. • Russia does not have an effective and publicly-known mechanism for the purpose of considering de-listing requests. • Russia does not have an effective and publicly-known procedure for unfreezing the funds of persons inadvertently affected by a freezing action.

2.5 The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and Analysis

195. Established at the end of 2001 as the Financial Monitoring Committee (FMC) by a Presidential Decree[32], the Russian FIU, now called the Federal Financial Monitoring Service or *Rosfinmonitoring*, is the central authority for combating ML and TF. It has been a member of the Egmont Group since June 2002 and operates according to the Egmont Group Documents[33]. Its powers and duties were confirmed in the current AML/CFT Law (article 8). Originally created as an independent government authority in 2001, Rosfinmonitoring was integrated into the management structure of the MoF in March 2004. In September 2007, Rosfinmonitoring was placed directly under the authority of the Prime Minister, though Rosfinmonitoring still enjoys full operational autonomy[34].

196. Rosfinmonitoring has in total 42 powers and duties, listed in Section II of the Rosfinmonitoring Regulations[35]. The most important of these are:

- Central (policy) co-ordinating body for AML/CFT issues.
- Collecting, processing and analysing the information about transactions which are subject to monitoring by designated reporting entities, and requesting further information about these transactions.

[32] Presidential Decree of 01.11.2001 no. 1263 "On the Authorised Agency for Combating Laundering (Legalisation) of Proceeds from Crime and Financing of Terrorism".

[33] Egmont Group Statement of Purpose and Egmont Group Principles for Information Exchange Between Financial Intelligence Units for Money Laundering, both implemented by Government Decision of 07.10.2002 no. 1405-r

[34] Presidential Decree no. 1263.

[35] Government Decision of 23.06.2004 no. 307 approved the Regulations on Rosfinmonitoring.

- Creation of a uniform information system and administering and maintaining the federal AML/CFT database, in line with data protection and secrecy provisions.
- Referring relevant information to the various law enforcement bodies when there is a suspicion of ML or TF. This happens upon request of the law enforcement authorities as well as upon the own initiative of Rosfinmonitoring.
- Carrying out co-operation and exchange of information with competent authorities of other countries in the AML/CFT sphere in accordance with international agreements of Russia.
- Representing Russia in international organisations on issues of combating money laundering and financing of terrorism.

197. Reporting entities can submit reports electronically to Rosfinmonitoring. The Russian authorities indicated that improvements to the IT systems used to receive and process transaction reports from reporting institutions, as well as co-operation with the BoR, other supervisors and professional associations of reporting institutions improved the quality of STRs. While in 2005 2.27% of all reports were rejected upon receipt, in 2007 this had dropped to 0.33%. CIs use the IT network infrastructure of the BoR to send reports to Rosfinmonitoring. The information is encrypted, and the BoR has no access to any of the data that pass through its IT system to Rosfinmonitoring.

Receiving and analysing STRs

198. After an STR is received, the Rosfinmonitoring IT system checks whether the report is complete. Incomplete reports are sent back. Reporting entities receive a notification to inform them about the detected deficiencies, after which they have to resubmit the report within 24 hours. If a report does not have any deficiencies, a reporting entity receives a notification on acceptance of the report by Rosfinmonitoring. Rosfinmonitoring drafts lists of most frequent mistakes by reporting entities and sends those to supervisory authorities. Rosfinmonitoring staff also contact reporting agencies directly if necessary to point out (technical) mistakes made.

199. During the second stage, data mining takes place. All the STRs are analysed by a software system. With the use of algorithms, reports are grouped based on different criteria, such as suspected person, nature of the operation and regional risks. Further on, reports are analysed for further investigation. External databases are also checked for additional information, this includes the databases of FCS, FTS, BoR, FSFM, Rosstatistics, Rossport, Assay Chamber, MIA, FSB, FMS, MoJ (and others). If necessary, additional information is requested, including information on other subjects revealed during the analysis of the reports. Thereafter, Rosfinmonitoring forwards the relevant information to law enforcement authorities according to their jurisdiction. All reports received by Rosfinmonitoring are kept in the Rosfinmonitoring database and used on the daily basis for analysis and intelligence purposes. The information sent to law enforcement can (in principle) be used in court.

Guidance

200. Most guidance is issued by Rosfinmonitoring on the basis of the AML/CFT Law (article 7). The Reporting Instruction[36] (RI) is the most current guidance for designated entities on how to report suspicious transactions. The RI establishes a single reporting format, includes reporting codes that can be used, defines communication protocols, lists and establishes templates for written requests by Rosfinmonitoring to reporting entities and a list of the officials that have the right to send written requests. For credit institutions, the RI is first approved by the BoR.

201. Rosfinmonitoring has issued reports about its activities since 2004. These reports include statistical data and information about:

[36] Rosfinmonitoring Order of 07.06.2005 no. 86 approved the Instruction "On Submitting to Rosfinmonitoring Information Stipulated in the Federal Law "On Combating Legalisation (Laundering) of Proceeds from Crime and Financing of Terrorism".

- Legal developments.
- Information technology and data transactions developments.
- Supervision activities, in particular: interaction with supervisory agencies, interaction between financial institutions and other organisations with supervisory agencies with Rosfinmonitoring, information on audits of organisations under the supervision of Rosfinmonitoring.
- Financial investigations.
- Money laundering typologies.
- Information on combating terrorism financing.
- International co-operation, including interaction between Rosfinmonitoring and the FIUs of foreign countries.
- Inter-agency co-ordination and interaction.
- The work of Rosfinmonitoring regional offices.
- Staffing support and personnel training.

202. Rosfinmonitoring provides guidance to reporting entities which includes explanation of the legislation and description of the legal developments. Furthermore the FIU gives training to reporting entities and participates in seminars where examples of ML cases are provided.

203. Rosfinmonitoring provides law enforcement agencies with information / typologies on a regular basis.

Access to information

204. The basic principle for Rosfinmonitoring to gain access to other agencies' information is laid down in the AML/CFT Law. All government entities (federal and regional) are required to provide all information and documents to Rosfinmonitoring that it needs to fulfil its duties, with the exception of information on the private life of citizens (personal and family life, such as religious beliefs, hobbies, letters, telephone conversations), unless overruled by court order in specific cases (AML/CFT Law, article 9).

205. The same article also indicates that any sharing of information is subject to restrictive conditions. Moreover, the AML/CFT Law also provides that any information sharing practice or procedure should not be in violation of existing secrecy provisions relating to banking, tax, official government information, commercial information, and communication. Communication secrecy explicitly extends to remittance of monetary funds.

206. One of the Regulations concerning the FIU[37] establishes the duty for all federal and regional bodies that register or license any of the designated financial institutions or DNFBPs to share updated lists of registered and licensed entities with Rosfinmonitoring on a monthly basis. Rosfinmonitoring also has direct access to these databases, in case of the register for commercial legal entities (maintained by the FTS), the access is on-line.

207. Rosfinmonitoring has information about lost passports and passport forms, and passports of deceased citizens. The list is updated every six months and is made available to reporting entities.

[37] Government Decision of 14.06.2002 no. 425, approval of the "Regulation on the submission of information and documents to Rosfinmonitoring by state bodies, state bodies Federal Subjects and local self-government bodies".

208. Having direct access by Rosfinmonitoring to other agencies' databases is possible; however, it requires an agreement with the other government authority. Rosfinmonitoring has concluded 12 such agreements, in which the owner of the database stipulates the conditions for Rosfinmonitoring to have access[38].

209. When analysing reports, Rosfinmonitoring can verify the information it received by sending a request to another federal or regional government body. Such a request can also be sent to a federal or regional government body on request from or on behalf of a foreign body involved in the fight against ML and TF (a rogatory letter or written request is necessary). Rosfinmonitoring reports that several thousand such requests are sent annually to other agencies and most of these requests are said to be answered within ten days (as set by law)[39]. Rosfinmonitoring can also send these requests to other federal executive bodies to support its own work, such as collecting statistics and analytical material.

Request for additional information from reporting entities

210. The FIU has the right to request additional information from the reporting entity[40], in order to verify the accuracy of the information obtained and to detect (other) ML/FT transactions or activities. Rosfinmonitoring sends written requests to reporting entities and asks for more information on the transaction or requests duly notarised copies of specific documents. This has been done in 90% of all financial investigations in order to check the hypotheses set up in the course of the FIU's research. In addition, on a regular basis there are "hot-line" phone calls to reporting entities that need to explain the information submitted to Rosfinmonitoring.

211. Reporting entities are required to answer Rosfinmonitoring within five working days after receiving the request, but Rosfinmonitoring may change this deadline if necessary. Reporting entities have the right, but not the duty, to submit additional information (beyond what is requested) to Rosfinmonitoring, if the reporting entity deems this necessary for the effective enforcement of the AML/CFT Law.

Dissemination of information and operational independence

212. Law enforcement bodies are obligated to provide feedback to the FIU on any case they receive from Rosfinmonitoring, although in practice it seems that law enforcement is reluctant to provide such feedback. Law enforcement bodies may also send a request to the FIU to receive information on transactions held in the database[41].

213. Until very recently only the central office of Rosfinmonitoring had access to the whole database of reports obtained. But now the regional offices also have access to the whole database and they can use all the data to carry out analysis (through VIPNET[42]). This is an improvement, as in the very recent past, the regional offices only had access to the data concerning their region. VIPNET is also used for operational communication between the headquarters and regional bodies. For official documents that cannot be sent electronically through VIPNET, information sharing between the headquarters of Rosfinmonitoring and the regional offices is done by secure government courier.

214. The decision to forward material to law enforcement bodies is taken by the head of Rosfinmonitoring, on the advice of the Expert Council of the unit. The representatives of the regional offices take part in its meetings when presenting their own cases.

---

38 Agreements have been concluded with the following agencies: BoR, FCS, FSB, FSFM, Federal Migration Service, MIA, MoJ, Ministry of Transport, FTS, ROSCOM, Rosstat, and Assay Chamber.

39 Government Decision, no. 425 d.d. 14.06.2002

40 AML/CFT Law article 7 and government decisions 307 and 245.

41 Article 8 of Federal Law no. 115-FZ, Government Decision no. 307, and Government Decision no. 425 of 14.06.2002.

42 VIPNET is a secure telecommunication network, isolated from other networks.

215. Data at the FIU is securely protected and only disseminated in accordance with the law. The Criminal Code establishes liability (including imprisonment for up to ten years) for any breach of secrecy by any employee of the FIU.

216. Rosfinmonitoring pays much attention to ensure the security of information. For this, the FIU approved an internal paper ("A framework of communication and information security support"), which determines possible threats to the security of information contained in the FIU database (the Unified Information System of the Service) and ways to combat these threats. In addition, in April 2006, the Department of Security and Protection of Information, a new autonomous department within the FIU was created. This department monitors all actions of users, has created alarms to detect intruders and a system that analyses the level of protection. A variety of firewalls have been created to protect the database from illegal access. All this is set up to ensure that the information from reporting entities that contains commercial, banking, tax and other secrets, is protected as much as possible.

217. Operational independence for the FIU is safeguarded by the AML/CFT Law and Presidential Decree N1263 which establish the FIU ("the authorised body") as a federal executive authority. This term is linked to a government Decision which states that all federal executive bodies are independent in exercising their authority established by federal laws, acts of the President and rules of the government[43]. Before this government Decision was issued in January 2005, the Chairman of the FIU was the first deputy minister of Finance, which was another way of ensuring operational independence.

Resources and internal organisation (Recommendation 30)

218. As with many Russian authorities, Rosfinmonitoring has organised its activities in a headquarters in Moscow and regional offices throughout the country. Rosfinmonitoring currently has seven regional offices, formally called Interregional Departments, in every one of the seven Federal Districts[44].

219. Budget and maximum number of staff is set by law (budget) or regulation[45] (staffing and organisation). The budget of Rosfinmonitoring has been growing over the last years, from RUB 470 million in 2005, to RUB 659 million in 2006 and RUB 764 million in 2007. The maximum number of staff since December 2005 is 350 for the headquarters (actual staff 305) and 295 in total for the seven regional offices (actual staff for the regions is 245). Before December 2005, the maximum number of staff was 250 for the headquarters and 155 for the regional offices. The table below provides for an overview of current maximum and actual staff numbers.

[43] AML/CFT Law article 3 and Standard Regulation on Interaction of the Federal Executive Bodies approved by Russian government Decision of 19.01.2005 no. 30.

[44] The 7 Federal Districts are (acronym and administrative centre within brackets): Central* (CFD, Moscow), North-West (NWFD, Saint-Petersburg), Southern* (SFD, Rostov-na-Donu), Volga* (VFD, Nizhny Novgorod), Ural (UFD, Yekaterinburg), Siberian* (SiFD, Novosibirsk) and Far Eastern* (FEFD, Khabarovsk). Districts with * have been visited by the evaluation team.

[45] Government Decision of 05.12.2005 no. 714.

Overview of staff at Rosfinmonitoring (as of January 2008)												
Office	**Total staff**			**Of which analysts**			**Of which supervisors[46]**			**Of which other staff**		
	max.	**actual**	**vacant**	**max.**	**actual**	**vacant**	**max.**	**actual**	**Vacant**	**max.**	**actual**	**vacant**
HQ	350	305	45	141	133	8	21	17	4	188	155	33
CFD	45	32	13	22	14	8	13	10	3	10	8	2
NWFD	41	31	10	20	14	6	11	10	1	10	7	3
VFD	42	37	5	20	17	3	10	10	0	12	10	2
SFD	52	44	8	32	24	8	11	11	0	9	9	0
UFD	37	33	4	19	16	3	8	7	1	10	10	0
SiFD	41	37	4	21	18	3	11	10	1	9	9	0
FEFD	37	31	6	19	17	2	9	7	2	9	7	2
Total	**645**	**550**	**95**	**294**	**253**	**41**	**94**	**82**	**12**	**257**	**215**	**42**

220. Rosfinmonitoring is allowed to establish up to 12 departments at its headquarters to ensure that its key responsibilities are properly carried out. While the number of departments is set by the government (which could have been considered a breach of the operational independence of Rosfinmonitoring if it were not for the fact that this is part of the government budget planning cycle), the FIU is allowed to adjust these numbers. The 10 departments that exist at this moment are:.

- Research and analytical departments.
- The Department for Financial Investigation.
- The Department for Combating Terrorism Financing.
- The Department for Planning, Administration and Co-ordination.
- The Information and Technological Department.
- The Department for International Relations.
- Supervisory department.
- The Department for Supervision Activities.
- Administrative departments.
- The Legal Department.
- The Executive and Financial Department.
- The Administrative and Personnel Department.
- The Department for Information Security and Protection of Information.

221. The Head of Rosfinmonitoring is also responsible for the organisation of the regional offices. He is empowered to create, reorganise or liquidate regional offices. The powers and rights and organisational issues of the regional offices are determined by regulation[47]. The regional offices interact with the authorities on the Federal District and Subject levels. Every regional office must have a department for supervision and a department for financial investigations. The co-operation between the headquarters and the regional offices is good, and the evaluation team did not detect any issues that

[46] Supervisory staff levels should be taken into account for Recommendation 24 (section 4.3), not for Recommendation 26.

[47] Regulation on the Territorial Body of Rosfinmonitoring, approved by MoF Order no. 127n (30.12.2004).

appear to impede efficient co-operation and co-ordination. Staff at headquarters and the regional offices have daily direct contact on any substantive matters. On the management level, there are video conferences on a weekly basis, or more often if required. At least once a year, the management of all regional bodies and the headquarters gather in Moscow. STRs are forwarded to law enforcement at the regional and headquarters level, to ensure that all levels involved are updated on actions taken and can follow up if appropriate.

222. Rosfinmonitoring is equipped with modern high-capacity equipment and appropriate software, enabling it to collect, analyse, store and disseminate a large number of STRs on an ongoing basis. Since mid-2004, Rosfinmonitoring receives about 10 000 to 12 000 messages per day (including STRs). The technical infrastructure makes it possible to use the most modern data processing software for handling data, supporting management decisions, permitting staff to work on specific cases and protecting information.

223. Up to 95% of the disclosures are submitted to Rosfinmonitoring in electronic form, which substantially facilitates both the transfer and acceptance of information. Reporting entities and other organisations can use special software to communicate with and send STRs to Rosfinmonitoring, all in real-time and free of charge. Financial institutions can thus transfer encoded messages through secured communication channels, signed with an electronic digital signature or PIN code.

224. The amount of data collected by Rosfinmonitoring has expanded by 80% since 2004. By January 2005, the FIU had received 3 million messages (including about 1.8 million STRs). In 2006, the database volume doubled when the FIU received another 6.1 million messages (3.8 million STRs). By April 2007, the database had accumulated about 14 million messages and STRs. All these data are subject to monitoring but are also used as intelligence for the FIU.

Professional standards

225. In addition to general requirements of the Russian civil service, Rosfinmonitoring has drafted special rules for hiring its employees[48]. These rules list for every staff level in a detailed way what the necessary knowledge, skills and education should be. Since 2005 the FIU welcomed 40% new staff at its headquarters and 90% new staff at its regional offices, and many resources were spent to ensure the hiring of quality staff. Currently, most employees of Rosfinmonitoring have a higher education, and 7% of them have scientific degrees. Confidentiality of staff is determined by law[49]. In 2006 the internal control systems detected an attempt of one of the employees of Rosfinmonitoring to check personal data of a case which he was not working on. Disciplinary sanctions were applied and the employee was fired. There were two other unauthorised attempts to access the database. These attempts were detected by the control system at the initial stages before any information had been disclosed.

Training

226. Since December 2005, all training for FIU staff is given based on a new system, in order to introduce a certain planned character and predictability in the professional training of all FIU staff (headquarters and regional offices). Basic training is given to all staff every three years, and work related training is given annually to all staff (although only 14 staff have been trained in 2007); 56

[48] "On the qualifying requirements regarding the professional knowledge and skills that are necessary for the fulfilment of work-related obligations by state civil servants of Rosfinmonitoring", approved by Rosfinmonitoring Order of 25.12.2006 no. 224. And "the Bylaw of the contest commission of the central office of Rosfinmonitoring for the conduct of the contest for filling a vacant position of the federal state civil service in the central office of Rosfinmonitoring and the method of conducting a contest for filling a vacant position of the federal state civil service in the central office of Rosfinmonitoring" approved by Rosfinmonitoring Order of 09.10.2006 no. 156.

[49] AML/CFT Law, article 8, and Federal Law of 27.07.2004 no. 79-FZ "On the State Civil Service" article 15, part 1, sub item 7 and sub clause 9.

other employees have received special courses in 2007. Headquarters staff are responsible for training of staff at regional offices (training seminars). All new staff get introduction training and a mentor.

227. Rosfinmonitoring recently created the Institute of Financial and Economic Security at the Moscow Engineering Physics Institute (MEPHI). The training institute is meant to provide training for AML/CFT specialists. The first trainees were selected by mid-2006 and the first graduating class is expected in 2008.

228. Another institute, the non-commercial International Training and Methodological Centre for Financial Monitoring (ANO-Centre), was created in December 2005. It has already provided 30 training seminars to over 2000 professionals from Rosfinmonitoring, supervisors, law enforcement and private sector employees from Russia and all other EAG countries.

229. The European Commission has also provided training for many employees of Rosfinmonitoring (and law enforcement and supervisory bodies) within the framework of Council of Europe project MOLI-RU (2003-2005) and MOLI-RU-2 (2007-2009).

Statistics

230. Rosfinmonitoring keeps a number of detailed statistics. The following represents the most important statistics that were provided to the evaluation team. Statistics are broken down on the type of reporting entity. More detailed figures can be found in section 3.7 of this report.

Statistic on reports received by the FIU 2003 – 2006		
	Year	**Number**
Number of STRs received by the FIU	2003	303 900
	2004	658 000
	2005	1 545 500
	2006	3 777 300
	Total	**6 284 700**
All reports received by the FIU (incl. STRs)	2003	974 873
	2004	1 772 595
	2005	3 053 382
	2006	6 147 974
	Total	**11 948 824**
Number of STRs transferred to law enforcement	2003	18 000
	2004	12 000
	2005	80 000
	2006	122 000
	Total	**232 000**

231. Russia does not keep full statistics on the number of STRs that result in investigation, prosecution and conviction. This is largely due to the fact that FIU information is mixed with other information at the law enforcement and prosecution stages. Nonetheless, Russia does have information on the number of cases that contain material from Rosfinmonitoring.

Statistic on criminal cases containing FIU material FIU 2003 – 2006		
	Year	**Number**
Number of ML investigations (law enforcement / prosecution) containing FIU material	2003	22
	2004	540
	2005	1 300
	2006	2 103
	Total	**3 965**
Number of TF investigations (law enforcement / prosecution) containing FIU material	2003	no data
	2004	no data
	2005	no data
	2006	7
	Total	**7**
Number of ML cases containing FIU material transferred to court	2003	1
	2004	2
	2005	35
	2006	208
	Total	**246**
Number of convictions for ML in cases containing FIU material	2003	4
	2004	9
	2005	16
	2006	95
	Total	**124**

Effectiveness

232. Rosfinmonitoring functions effectively.

2.5.2 Recommendations and Comments

233. Rosfinmonitoring meets Recommendation 26. Nevertheless, the number of vacancies is somewhat high and the evaluation team considers that all vacancies should be filled.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**C**	• This Recommendation is fully observed.

2.6 Law enforcement, prosecution and other competent authorities – the framework for the investigation and prosecution of offences, and for confiscation and freezing (R.27 & 28)

2.6.1 Description and Analysis

Recommendation 27 (Designated law enforcement and prosecution authorities)

234. The main law enforcement bodies concerned with the fight against ML and TF are the Ministry of Internal Affairs (MIA), the Federal Security Service (FSB), the Federal Service for the

Control of Narcotics Circulation (FSKN), and the Prosecution Authority. These bodies have all been established by law, as are their activities[50]. The responsibility for ML investigation and prosecution is established in the CCP which stipulates that preliminary investigation on money laundering and self laundering is conducted by MIA investigators. The responsibility for TF investigation/prosecution is also regulated in the CCP, which stipulates that preliminary investigation on terrorist financing cases can be conducted by the Prosecution Authority, the FSB and MIA. The FSKN is the competent authority in all ML and TF cases as long as drugs are involved [CCP article 151(3-2), 151 (a-1-2), 151(a-2-2), CC article 174, 174.1 and 205-1].

Ministry of Internal Affairs (MIA)

235. The Ministry of Internal Affairs (MIA), also known by its Russian acronym MVD (*Ministerstvo Vnutrennikh Del*) is the main law enforcement body of Russia. The principal units of the MIA are the regular police (*Militsiya*), the Road or Traffic Police (State Road Inspection Service), and the Internal Troops. Since the disbanding of the Tax Police, the MIA also investigates economic crimes. The main task of the MIA is the prevention, detection, suppression, disclosing and investigation of crimes.

236. The AML activities of the MIA are also guided by Presidential Decrees. The current three main ML priorities are set by the NASP:

- Organisational and methodological support, co-ordination of activity of police units of the Federal Subjects on fighting economic crime and tax crimes.
- Conducting investigations aimed at revealing crimes related to ML and TF.
- Organisation of interaction with Rosfinmonitoring, the FSB and other domestic and foreign law enforcement bodies.

237. The Investigation committee is an autonomous permanent unit of the central headquarters of the MIA that directs MIA's investigative bodies. The Investigation committee itself is supervised by the Prosecution Authority. There are several other bodies within the MIA that deal with ML/TF issues, such as the Department of Economic Security (DES), the Department on Combating Organised Crime and Terrorism, the Department on Ensuring Legal Order on Transport, the Department on Ensuring Legal Order in Closed and Regime Territories of the MIA, the Investigative Committee, and the Central Command of Internal Troops.

238. DES co-ordinates MIA's activity in revealing, suppressing, and investigating crimes related to money laundering. The maximum number of staff for all units of DES is 18 400, which includes 368 specialised AML/CFT officers. Each preliminary investigation unit of each of the Federal Subjects has a specialised unit for investigation of economic crimes. Every of these units employs two to three ML investigators, but other experienced officers can also lead and handle ML cases. For large criminal investigations relating to a variety of crimes, investigative groups are formed.

Federal Security Service (FSB)

239. The Federal Security Service (FSB) is Russia's domestic federal and intelligence security service. The FSB Law[51] sets out the main objectives, structures and the legal basis for its activities, its responsibilities, resources, as well as the rules for its control and supervision. The FSB Law states that the FSB is active in the following areas (although other areas can be added by federal law):

[50] Such as the Criminal Code, Code of Criminal Procedure, along with the Federal Laws "On Operational Search Activities," "On Combating Extremist Activities," "On Combating Terrorism," "On the Federal Security Service," "On Foreign Intelligence," the laws "On Security," and "On Militia".

[51] Federal Law no. 40-FZ "On Federal Security Service" of 3.04.1995.

- Counter-intelligence activity.
- Combating terrorism.
- Combating criminality.
- Intelligence activity.
- Protection of state borders, inland sea waters, and natural resources.
- Provision of information security.

240. The main goals of the FSB are to combat organised crime, corruption, smuggling, money laundering, terrorism, illegal migration, and illegal traffic in weapons, ammunition, explosives, drugs and psychotropic substances. The FSB can deploy special technical equipment to gather intelligence to combat extremist activity, separatists, illegal armed forces, criminal organisations and groups or entities that aim to overthrow the government. Overall, for most types of crimes, the FSB would focus on the most dangerous or threatening crimes, criminals and criminal groups.

Federal Service for the Control of Narcotics Circulation (FSKN)

241. The Federal Service for the Control of Narcotics Circulation (FSKN) is the main federal authority in the fight against illegal trafficking of drugs. In addition, it also develops state policies, drafts legal regulations, controls and supervises (legal) drugs, psychotropic substances and precursors and their circulation in Russia[52]. If the FSKN investigates a predicate offence for ML, it will always include an investigation for ML. However, the FSKN has some problems in conducting ML cases due to the fact that ML is usually part of complex cases and is only a secondary crime for the FSKN.

242. Within the FSKN, the Operational Search Department (created in 2004) includes the Bureau on Undermining the Economic Basis of Drugs Crimes. The primary goals of this department are:

- Detecting, prevention, suppression and disclosing ML, also by organised criminal groups / associations.
- Participation in development and implementation of state policy in the area of combating illegal drug traffic.
- Management and co-ordination of activities of operative divisions of the FSKN.

The Prosecution Authority

243. Russia has a centralised federal-level prosecution system. Every prosecutor in Russia is subordinate to the Prosecutor General. The Prosecution Authority is independent from the executive, legislative and judicial branches. The structure, function and operational independence is provided for by the law, as is the procedure through which prosecutors are appointed[53]. The evaluators found that, generally, the prosecutors are able to perform their work in the area of ML and TF independently.

244. The relevant federal law lists a variety of tasks for the Prosecution Authority[54]. The most important for this report are the duty of criminal prosecution and the supervision over and co-ordination of investigative control activities of law enforcement bodies, especially to ensure that law enforcement bodies obey the law. However apart from this, the Prosecution Authority also has direct

[52] Regulation "Federal Service on Control of Narcotics Circulation", approved by Presidential Decree no. 976 of 28.07.2004.

[53] Article 129 of the Constitution and Federal Law no. 2202-1 of 17.01.1992 on the Prosecution Office.

[54] Federal Law 2202-1 «On Prosecution Office » as of 17.01.1992.

investigative powers (or prejudicial powers) in relation to some offences, including ML and TF (article 151, item 2, sub-item 1 from CCP).

245. The main departments within the General Prosecution Office are: the Department on supervision over the investigation, the Department on supervision over inquiry and the Department on supervision over execution of the legislation on combating corruption, and other units. This last department (established in August 2007) also carries out the supervision over preliminary investigation of ML cases. Any law enforcement body that starts an investigation has to inform the Prosecution Authority within 24 hours. The Prosecution Authority claims that this system enables them to be aware of all ongoing cases. However, the evaluators repeatedly noted during various on-site meetings in the regions that the Prosecution Authority officers present were often not completely knowledgeable about all cases, for example, regarding corruption and bribery in Customs and Federal Migration Service in the same regions.

246. The Prosecution Authority can refer ML cases back to law enforcement, especially to ask for additional evidence in instances in which procedures have been violated. All regions follow the same practice; one region claimed that this happens quite often and mostly because of lack of quality of the ML cases it had received. However, the evaluators also note that lack of quality of ML cases by law enforcement points to a lack of supervision by the Prosecution Authority. This might be a problem, as with the rise in the ML case-load there is a proportionate increase in the numbers in returned cases[55].

247. In addition, the Constitution stipulates that the Prosecution Authority is tasked with the supervision (or "enforcement") of the law[56]. This is a general rule that has been repeated in several specific laws, such as the AML/CFT Law, which states that the Prosecution Authority should have oversight over the AML/CFT Law, which includes supervision of designated entities (article 14). This however refers to a general duty of the Prosecution Authority to investigate criminal violations of the law, and it does not relate to the supervision of compliance as defined in the FATF Recommendations although information provided to the evaluators some time after the on-site visit(s) suggests that the Prosecution Authority has a limited role in supervision (see section 4.1). Other forms of supervision duties are related to observance of human and citizens' rights and freedoms and to observance of the law by administrations of the bodies and institutions responsible for executing sentences and sanctions ordered by court and by the administrations dealing with detention and custody facilities.

Corruption (effectiveness)(relating to all law enforcement bodies)

248. Corruption is a problem in Russia and it certainly does have a negative impact on law enforcement, as described in section 1 of this report. Even though law enforcement staff are currently better paid than immediately after the independence of Russia and during the 1990s, underpaid law enforcement staff are still very much vulnerable to corruption. Low salaries also cause trained and experienced staff to leave the service and to join private sector companies. This causes the lack of funding of law enforcement to weaken the overall effectiveness of the AML/CFT system to a great degree. The exception in this case seems to be the staff of the FSB, which are better paid than other law enforcement staff.

[55] The number of ML cases returned to MIA rose from 106 in 2004 to 242 in 2005 and topped 385 in 2006. The number of ML cases returned to the FSKN grew from 2 in 2004, to 31 in 2005 and reached 61 in 2006.

[56] Federal Law 2201-1, section 3, chapter 1; and the Constitution.

Powers to postpone or waive arrest or seizures

249. Russia has taken measures that allow the investigative officer (law enforcement) or the supervising prosecutor to postpone or waive the arrest of suspected persons or the seizure of criminal money. This is all part of the regular evidence building process and can be used when investigating ML, TF or predicate offences[57].

Additional elements

250. According to the law on Operational Search Activities, law enforcement and Prosecution Authority are able to use a wide range of special investigative techniques, such as interrogation, making inquires, collection of samples for a comparative study, test purchases, examination of premises, buildings and vehicles, examination of items and of documents, surveillance, identification of persons, mail, phone and internet, wiretapping of telephone conversations, and saving all information through communication channels, undercover operations, controlled delivery and so on. The law is very flexible since it does not lay down comprehensive restrictions concerning the use of these measures, for example regarding their period of applicability or the type of offences concerned. These measures can be used for ML, TF and predicate offences, by single law enforcement departments or by investigative groups, who can all use all measures (based on their assessment of their needs).

251. Investigative groups that use these investigative techniques do not solely consist of ML or TF specialists, and those that investigate predicate offences will always take the lead in any investigation. Investigative groups can become joint investigations with other countries, provided it is done on the basis of a treaty or agreement. Russia has taken part in joint investigations, for example with CIS countries, Switzerland and the United States. ML methods and techniques are studied by law enforcement and FIU.

Recommendation 28 (Law enforcement powers)

252. All law enforcement agencies are authorised to use a wide range of powers when conducting investigations of money laundering, terrorist financing and predicate offences. These powers include: *i)* the compulsory acquisition (*i.e.* inquiry and detention) of articles, documents and other materials relevant to the crimes; *ii)* the search of persons, articles, houses and other premises where suspects or criminal evidence may be hidden; and *iii)* the seizure and acquisition of articles relevant to the crimes.

253. To exercise most of these powers, law enforcement investigators do not need a court order. In specific cases however, the Prosecution Authority must approve, and a court order is required. This applies for search of private homes and the seizure of subjects and documents containing information on deposits and accounts in banks and other credit institutions, if the information is protected by confidentiality and secrecy provisions. These powers also apply to investigations and prosecution of ML, TF and predicate crimes and in relation to freezing and confiscating the proceeds of crime. None of the officials whom the evaluators met with made any reference to any particular difficulty to use any of the provisions [CCP, articles 165 and 29(2/4-9&11)].

254. The power to take witness statements is based on the CCP. A witness can be any person who may know any circumstances that are important for investigation and who has been called to provide evidence. Witness statements can be used in ML, TF and predicate offence cases by all law enforcement authorities when investigating a case (CCP, articles 56 and 187 – 194).

[57] CCP, article 38(3-2) and the Federal law no144-FZ on operational search activities (12.08.1995) article 11.

Resources and professional standards (Recommendation 30)

255. All law enforcement staff that the evaluation team met with expressed satisfaction with their working conditions, means and resources available, although that is the case for every single government authority that the evaluation team met with in Russia. The Department of Economic Security within the MIA has a staff of 18 400, including 368 officers working in the specialised AML/CFT division. The Directorate for Tax Crime has a total of 11 000 officers that could be involved in ML cases. In three of the visited regions (Khabarovsk, Kaliningrad and Rostov-na-Donu,) the number of police officers involved in ML and TF cases seems to be sufficient compared to the number of initiated criminal cases. For example, in the Rostov region, during the on-site visit there were 41 ongoing ML cases and another 162 investigations based on STRs received from regional Rosfinmonitoring offices. These cases were handled by over 300 police officers involved in investigation departments and 116 police officers working in operational search departments. In Kaliningrad, the number of staff in investigative divisions is 399 who detected 156 ML offences between 2003 and 2007 (mostly in 2007), of which 71 reached the courts. In Khabarovsk, 90 police officers are involved in economic crimes. In 2006, these officers detected 23 ML offences, of which 19 were submitted to court. So far, three cases have resulted in imprisonment and 2 cases in a fine.

256. The staff of the FSKN is 1 400 at the headquarters (officers and civil staff) and 40 000 overall. No information could be provided on the number of staff actually concerned with ML and TF, as information on the specific deployment of FSKN staff is considered a state secret[58]. The budget of the FSKN for 2007 amounted to RUB 14.1 billion, almost double from 2004[59]. The FSKN enjoys the same level of operation independence as other law enforcement bodies. The number of ML cases handled by the FSKN has been stable for the last few years. About 2 733 cases have been under investigation, of which around 1 592 have been closed and 1 494 sent to courts**.**

257. The FSB seems to be effectively organised. As with other law enforcement bodies, the FSB seems to have sufficient independence. However, no information was given on the operational independence of investigative staff or groups within the FSB, on the number of staff (overall and devoted to ML and TF), the annual funding, the number and nature of cases undertaken. All this is considered to be highly confidential, even though in relation to ML, the FSB is a regular law enforcement body. The law enforcement activities of the FSB focus on detecting, preventing, suppressing and disclosing espionage, terrorism, organised crime, corruption, illegal arms and drugs circulation, smuggling, if those present a threat to the security of the country[60].

258. Russia indicated that the special divisions of the MIA that are responsible for AML/CFT, are staffed through special selection of officers that have to meet high professional requirements imposed. The corresponding regulation[61], however, was not available, and no information was given as to its content. Apart from that, MIA employees must adhere to secrecy provisions, a rule that applies also to other law enforcement bodies (FSB, FSKN and the Prosecution Authority) as well. All law enforcement staff are bound by human rights provisions, such as the prohibition against abuse of power[62]. Both MIA and FSB staff can be held responsible for any misuse of powers.

259. Rules for the Prosecution Authority can be found in the Prosecution Law. Prosecutors need a university degree in law, enjoy to a high degree a *de facto* immunity from prosecution for a crime, cannot work in close relationship with a family member and must agree to a background security check (Prosecution Law, article 40.1). As of October 2007, the total number of prosecution officers (operational staff) was 29 380 for Russia and 1 028 for Moscow only. In the headquarters, 43 staff

58 Article 5 of Law no. 5485-1 of 21.07.1993 "On State Secrecy".

59 The budget for 2006 was RUB 12 billion, for 2005 – RUB 9.7 billion and for 2004 – RUB 7.7 billion.

60 Article 10 of Federal law no. 40-FZ "On federal security service" of 03.04.1995.

61 Resolution 4202-1 of the Supreme Soviet of Russia of 23.12.1992 «On Approval of the Regulation on Service in Law Enforcement Agencies and the Text of the Oath of the Officer of the Law Enforcement Agencies.

62 See for examples of abuse that is prohibited by Russian law the corresponding articles 5, 6 and 7 of the European Human Rights Convention 1950.

were dealing with ML/TF issues, throughout the country, and another 500 staff were working on ML/TF. All prosecutors are allowed to investigate ML/FT cases. ML/FT cases that are investigated by other law enforcement bodies are supervised by the Prosecution Authority, based on a variety of criteria such as which law enforcement authorities is carrying out the investigation, the place of the crime and place of the preliminary investigation.

260. The professional requirements for FSB personnel are formulated broadly. The FSB Law indicates that any citizen of Russia capable in his personal and business qualities, age, education and health to execute entrusted duties can be appointed as an employee of the FSB. While in service, the staff are guided by the federal law only, are not allowed to be bound by decisions of political parties, mass movements and public associations. As with all state service employees, the law prohibits the staff of the FSB from engaging in business activity, or rendering assistance to businesses (FSB Law, article 16).

Training (Recommendation 30)

261. Considerable resources are spent on training within law enforcement. Various bodies within the MIA, such as the Investigative Committee, DES, the Academy of Management, the Nizhniy Novgorod MIA Academy and the MIA Scientific Institute, have developed over 50 methodologies for its staff, of which three[63] were presented to the evaluators. The objective is to enhance the detection, prevention, suppression and solution of crimes relating to money laundering. The MIA has also published evaluation reports and best practices on money laundering, to enhance the results of MIA staff in ML and related cases.

262. The MIA and its educational institutions have developed and organised a number of specialised courses on ML. For example, the MIA Economic Security Academy is in the process of establishing a new specialised training on ML. The MIA All-Russia Institute of Refresher Courses and the Nizhniy Novgorod and Volgograd based MIA Academies already have experience in providing ML and TF training and refresher courses. The MIA All-Russia Institute of Refresher Courses also provided a management level training for all the heads of Organised Crime and Terrorism Department Divisions. During this training, existing practices were evaluated, and proposals were made to improve the existing AML/CFT investigative practice. International training was part of the MOLI-RU and MOLI-RU-2 projects. However, the evaluators found that international training is not structurally provided for, at least not in the border regions (Khabarovsk since 1999 and Rostov since 2005). In addition, when queried by the evaluation team, many of the law enforcement representatives in the regions were confused as to the legal provisions of the ML law. For example, some did not realise that not all crimes are predicate offences for ML.

263. Those officers of the FSKN involved in economic crimes are trained on an ongoing basis by the FSKN Far Eastern and North-western Institutes of Refresher Courses. Training material on the following topics were developed:

- Use of e-payment systems for money laundering.
- Use of Internet as a source of information.
- Legalisation of proceeds from drugs through the real estate market.
- Use of bank cards in the field of illegal drug traffic.
- Use of money transfer systems without opening an account.

[63] "Legal aspects of interaction with Rosfinmonitoring in the field of combating money laundering"; "Organisational and practical aspects of interaction with Rosfinmonitoring in the field of combating money laundering"; and "Typologies of money laundering according to FATF experts".

264. ML and TF are a part of the initial FSB training as well as refresher courses. For example, the basic training course for new operational staff at the FSB Academy includes AML issues in the organised economic crime module. CFT knowledge is included in the module on organised terrorist activities. During refresher courses, these topics are studied in more depth by officers who serve in the economic security and combating terrorism units. During their service FSB staff are enrolled in additional training at the FSB Academy or at other FSB training facilities in Nizhniy Novgorod, Novosibirsk, Saint-Petersburg, Yekaterinburg and Moscow. The FSB Institute of New Information Technologies offers practical knowledge courses.

265. The Prosecution Authority trains its own staff. The Prosecution Law provides that training needs to be ongoing and that skills need to be upgraded on a continuous basis (article 43.4). The Russian authorities did not provide any other information concerning the practical implementation of this legal provision. The Prosecution Authority provides guidance manuals for investigation staff on money laundering, on banking and tax secrecy, and return of foreign currency from abroad.

Additional elements

266. AML/CFT training is also provided to the judiciary. In 2002, the general courts of first instance studied the legal implications of the money laundering provisions. A summary of this study was sent to the Presidential Executive Office. In 2004, the Supreme Court issued a guideline on how to handle ML criminalisation. Currently, a working group is studying the judicial practice in ML and TF cases. The results of this study will be made available to the FIU, courts and law enforcement agencies.

267. In order to improve operational and search activity and investigation practice, MIA, FSKN and FSB officers are said to evaluate and analyse their activities, define the most common "modus operandi" and high risk ML/TF corridors and regions. The output allows these services to build on typologies.

2.6.2 Recommendations and Comments

268. Overall, the system is in place and there is a continuous concern for improvements within all bodies and especially in the headquarters in Moscow. Still, there are some significant differences in the regions.

269. The MIA, FSKN, FSB and Prosecution Authority are all clearly responsible for ML/FT investigations. Nevertheless, the evaluators had difficulties in discovering which body would be responsible in each case. According to provisions of CCP, the Prosecution Authority has powers for transferring a case from one law enforcement body to another during the primary investigation. The evaluation team is not sure what the criteria are for transferring a case from one law enforcement body to another, but it seems that this practice has a negative impact on the effectiveness. Especially in the absence of specific legal provisions that determine the competences of each law enforcement body in ML/TF crimes. The initiation of a general discussion on how to define and determine the competences of law enforcement agencies and their specialised units would be beneficial.

270. One way to ensure a better distribution of work would be if the Prosecution Authority implemented more rigorous supervision, to at least to be able to be aware of all cases pursued by law enforcement bodies. Even though the Prosecution Authority claimed to be aware of all cases, when queried by the evaluators on specific cases, representatives met with often gave the impression of having limited knowledge. The supervision activity of Prosecution Authority seems not to be efficient for another reason. Too often the Prosecution Authority has to return cases to (other) law enforcement bodies for additional information, caused by lack of factual circumstances, not exhaustive research, breach of procedures, violation of rights etc. The fact that both the Prosecution Authority and law enforcement bodies indicated a lack of quality of cases raises concerns with the evaluators.

271. Corruption is a problem and it continues to be a problem for all law enforcement bodies. While the government is to be commended for its policy efforts to eliminate corruption, these efforts had an insufficient impact throughout the country. Unless Russia succeeds in eradicating corruption, its law enforcement bodies will continue to be less effective than possible.

272. The competent authorities appear to have all necessary powers in order to investigate money laundering, terrorist financing and other underlying predicate offences. The MIA, FSB and FSKN indicated that the powers specified in Recommendation 28 were often used in investigations of money laundering, terrorist financing and other predicate offences.

273. All law enforcement authorities should continue to strengthen the existing inter agency AML/CFT training programmes in order to have specialised financial investigators and experts at their disposal. Also, there is a need to enhance and implement international training programmes on ML and FT issues, especially for law enforcement staff in the (border) regions.

274. The low number of ML convictions in comparison with the number of detected ML crimes should be addressed and consideration should be given to a greater specialisation within the Prosecution Authority and the judiciary, including establishing specialised units within Prosecution Authority and specialised courts for ML and FT, in order to increase the effectiveness of the system.

2.6.3 Compliance with Recommendations 27 & 28

	Rating	Summary of factors relevant to s.2.6 underlying overall rating
R.27	**LC**	• The discretionary powers of the Prosecution Authority to transfer a case from one law enforcement to another may lead to a lack of clear distribution of money laundering cases among law enforcement bodies (effectiveness issue). • Corruption has an impact on the effectiveness of the system. • Some designated law enforcement bodies do not appear to have sufficient knowledge of the ML provisions.
R.28	**C**	• This Recommendation is fully observed.

2.7 Cross Border Declaration or Disclosure (SR.IX)

2.7.1 Description and Analysis

275. The Federal Customs Service (FCS) and the BoR share the responsibility for currency control issues in Russia, but the FCS has the sole responsibility for clearing and control at the borders. There is a regional FCS body in each of the 7 Federal Districts, and each Customs District is sub-divided into customs houses and customs stations[64]. Within The FCS, the Central Customs Clearance Administration and the Central Administration on Countering Smuggling are in charge of all matters relating to FATF Special Recommendation IX. The law enforcement units of the FCS are divided into operational divisions, research units and administrative investigations units. Their main task is to combat smuggling, other crimes and administrative customs offences, to suppress narcotics and arms trafficking, as well as assist in the fight against terrorism (article 403, Customs Code). Studying methods of crime to develop guidelines is another task for the FCS.

276. Russia has implemented a declaration system, which is not fully identical for incoming and outgoing passengers. The system is based on the Currency Control and Regulation Law[65] (CCRL).

[64] Central: 25 customs houses, 1 operation, 193 customs stations. North West: 19 customs houses, 22 operation 125 customs stations. Southern: 13 customs houses, 1 operation, 86 customs stations. Siberian: 16 customs houses, 2 operations, 80 customs stations. Volga: 15 customs body, 1 operation, 79 customs stations. Far East 15 customs houses, 1 operation, 56 customs stations. Ural: 9 customs houses, 1 operation, 60 customs stations. There are also 7 customs houses and 31 customs stations subordinated directly to the FCS.

[65] Law of 10.12.2003 no. 173-FZ on Currency Control and Currency Regulation.

This Law was adopted in 2003, and its aim was to consolidate Russia's monetary policy, in order to develop the Russian economy. AML/CFT was not one of its aims. The law has been amended a few times since then, and it now includes FATF Special Recommendation IX related provisions. However, the law does not contain any reference to ML or TF, and without knowledge about the legal history, front line officers of the FCS might not know what the purpose of these provisions is.

277. All incoming persons are obliged to declare any foreign or Russian currency in cash, as well as travellers' cheques and securities, if the amount exceeds the equivalent of USD 10 000 (CCRL, article 15). According to the same law, the term *securities* includes domestic security papers related to the securities market (article 1, part 1, item 3 of CCRL) and "other securities" which covers all other bearer negotiable instruments. External securities are defined as non domestic securities (article 1, part 1, item 4 of CCRL). However, the Russian version of the Customs declaration forms asks for the reporting of cash and *currency valuables*, while the English version asks for cash and securities, which is confusing. Despite this inconsistency in the implementation of the law at the border, the team considers that the law covers all bearer negotiable instruments. In order to increase effectiveness, Russia should streamline the Russian and English version of the Customs declaration form.

278. Outgoing travellers can freely take travellers' cheques and foreign or domestic securities with them, irrespective of the amount. Cash can be taken freely out of Russia if the amount does not exceed USD 3 000. Any amount between USD 3 000 and USD 10 000 must be declared, and the traveller does not have to prove that the cash was imported or wired into Russia before. The export of amounts exceeding USD 10 000 in foreign and domestic currency is prohibited, unless otherwise licensed on the incoming declaration form (CCRL, article 15). In addition, travellers' cheques below the threshold of USD 10 000 should be voluntarily declared[66]. Despite these specific rules for travellers' cheques, these are not mentioned on the Customs declaration forms.

279. Shipment of currency through containerised cargo is not covered, even though the authorities argue that the general provisions of the CCRL cover any import or export of cash. The mailing of cash is prohibited[67]. The evaluation team specifically asked Customs and Russia Post if systems are in place to detect currency transportation through mail and containerised cargo. The authorities stated that this is not the case and that it was not necessary, since money would be sent through money transfers.

Powers of competent authorities upon discovery of a false declaration/disclosure or suspicion of ML/FT

280. In case of a false declaration or non-declaration, a customs officer can initiate an administrative offence case (Code of Administrative Offences 15.25 and 16.4) or a criminal case if the value of the non-declared cash exceeds RUB 250 000 (article 188.1 CC) and require the traveller who attempts to unlawfully transport currency or securities to explain the origin and intended use of the cash. The questioning of the traveller can also be based on the urgent investigative powers of the FCS (CCP, article 151 and item 2 of Regulations on the Customs Investigation Administration). As a general power, FCS staff may also request relevant documents and information from travellers who move goods and vehicles across the border. The term *goods* is to be understood to include any movable property, including currency (Customs Code article 11.1).

66 CCRL article 15 item 3.1. and item 4.

67 Customs Code article 292.1.2 and 294.

281. If an administrative offence is detected, customs officers can withdraw or seize the instruments and objects used to commit the offence, as well as any related document[68]. If a criminal offence relating to articles 188, 189, 190, 193 or 194 (CC) is suspected, customs officers are entitled to use all powers of the CCP, which includes seizure of relevant items, however, in the context of this report it is important to note that articles 193 and 194 CC are not predicate offences for money laundering. Customs officers have no powers to stop or restrain declared currency or bearer negotiable instruments if there is a suspicion of money laundering. The customs officers may only monitor the suspects. This may be helpful in incoming cases, but monitoring persons that have left the country is impossible. The exception would be if a traveller is a designated terrorist entity (see section 2.4 of this report). The list with these entities is available to Customs.

Information collected, retained and shared

282. Customs keeps a database that holds all the declarations of incoming and outgoing currency of USD 10 000 or more. Access to this database is possible for authorised staff only. The database holds all the information that is submitted on the declaration form (incoming or outgoing, currency code, amount, form, and traveller identification data). Customs does not keep a separate database of suspicions of ML or TF based on cross border movement of cash or bearer negotiable instruments – such data could be found in regular law enforcement databases on a case by case basis. The Russian authorities indicated that the relevant information in the Customs database is shared with Rosfinmonitoring, tax authorities and law enforcement bodies based upon special agreements. The MOU between the FCS and Rosfinmonitoring enables the IT department of Rosfinmonitoring to link into the Customs database.

Co-ordination among domestic competent authorities

283. In addition to co-ordination with Rosfinmonitoring, Customs co-operates with the BoR, law enforcement bodies, tax authorities and the Federal Migration Service. To this end, joint investigation groups are formed. The authorities provided the evaluation team with an example of such a co-operation agreement, but the example that was provided concerned an investigation that falls outside the scope of this Special Recommendation.

International co-operation and assistance

284. Within the FCS, the Customs Co-operation Administration and the Smuggling Prevention Administration is responsible for international co-operation. The key objective is to co-ordinate the international activities of all entities within the FCS to ensure that the co-operation with foreign authorities and international organisations is in line with the policies of the FCS and the law. To this end international interagency agreements have been concluded with 13 countries,[69] and mutual customs assistance agreements have been concluded with 36 countries (three are currently under negotiation)[70].

---

[68] Code of Administrative Offences, article 15.25 (breach of the currency legislation of goods the Russian Federation and acts of currency regulation bodies) or 16.4 (Non-declaration or unreliable declaration of foreign currency or Russian currency by natural persons).

[69] Interagency agreements and protocols have been concluded with: China, Estonia, Finland, France, Hungary, Latvia, Lithuania, Mongolia, the Netherlands, Norway, Poland, Serbia (Federal Republic of Yugoslavia) and Sweden.

[70] Intergovernmental agreements have been concluded with (in chronologic order) Greece, Korea, Germany, Mongolia, Norway, Sweden, Finland, China, USA, Poland, Lithuania, Bulgaria, Serbia (Federal Republic of Yugoslavia), Israel, India, Denmark, Turkey, Slovakia, Czech Republic, France, Argentina, Hungary, Macedonia, Italy, Iran, Spain, the Netherlands, Estonia, Belgium, Brazil, Latvia, Chile, Mexico, DPRK, Romania and Columbia. Agreements are being negotiated with Albania, Croatia and Slovenia.

285. To improve co-operation, Russia operates representative offices in 7[71] countries. On the regional level, regions have also concluded agreements with neighbouring countries. The Kaliningrad region, for example, is co-operating with Estonia, Finland, Belarus, and Lithuania; the Khabarovsk region, with China, and the Rostov-na-Donu region co-operates with Ukraine. The FCS also presented examples of international co-operation cases to the evaluators. With regard to special operations, the FCS is empowered to exchange information internationally through the World Customs Organisation Regional Intelligence Liaison Offices system, which is protected from unauthorised access.

Sanctions

286. Administrative sanctions are available to deal with non-compliance of currency customs rules. The sanctions are listed in the table. The table does not include sanctions available for non-payment of customs taxes and duties on imported goods. Since the fines are connected to the minimum monthly wage, it is worth noting that the minimum monthly wage was RUB 1 100 between May 2006 and September 2007 and was raised to RUB 2 300 since then. This means, for example, that the maximum administrative sanction for a natural person non-declaring cross-border transportation is between USD 860 and USD 2 220 which is around eight to 20% of the smuggled amount. This is a rather low fine. The possible confiscation of the cash is not considered dissuasive, in particular not in cases where the cash or bearer negotiable instruments are smuggled on behalf of a third person who actually owns the money. Criminal sanctions for non-compliance with currency rules are also available (article 188.1 CC).

Sanctions for non-compliance with currency provisions			
Type of sanctions	**Description**	**Subject**	**Sanctions**
Administrative sanctions	Basic fines for non-compliance with any customs rule, except for false or non-declaration of cross border cash movement (AOL, article15.25.7)	Natural persons	Fine of 5 – 10 times minimum wage.
		Officials	Fine of 10 – 20 times minimum wage.
		Legal persons	Fine of 50 – 100 times minimum wage.
	False or non-declaration of cross border cash movement (AOL, article 16.4)	Natural persons	Fine of 10 – 25 times minimum wage.
Criminal sanctions	Smuggling (CC, article 188, item 1)	Natural persons	Between a fine of RUB 100 000 and five years imprisonment.

287. If a money laundering or terrorist financing offence is suspected or proven, all seizure and confiscation measures apply, as described in section 2.3 of this report. Shortcomings described in section 2.4 (Special Recommendation III, freezing of terrorist assets) have a negative impact.

Gold and silver

288. Precious metals and stones can be imported to Russia without any restrictions, although such imports are subject to import duties as with any other goods. Export of precious metals and stones is free for individual persons if for non-commercial use. If an illegal cross border movement of precious metal or stones is detected, a criminal case could be initiated, and Russia could send a mutual legal assistance request to another country, on a bilateral basis or through the World Customs Organisation Customs Enforcement Network. The authorities indicated that in 2006 – 2007, in 12 cases other European countries were notified, which led to concrete law enforcement results with two countries (Finland and Italy).

[71] Representations in: Belgium, Belarus, China, Finland, Germany, Kazakhstan and Kyrgyz Republic.

Safeguarding information

289. Customs data are protected by secrecy rules designed to protect from unauthorised access[72]. FCS information is stored encrypted and transmitted via secured channels. FCS has created internal security divisions responsible for safeguarding information; and in addition, every unit of the FCS has officially appointed officers responsible for the protection of information.

Additional elements

290. To detect illegal cross border transportation of cash, the Russian authorities indicate that x-ray and scanning equipment are used at its borders, passengers are questioned on a risk-based basis and on the basis of intelligence. Russian authorities consider elements of the Best Practice Paper for Special Recommendation IX to be implemented.

Resources and professional standards (Recommendation 30)

291. Russian authorities indicated that the law enforcement elements of the customs service are currently staffed at a sufficient level and have the necessary technical resources at their disposal. The FCS budget was increased from RUB 19 billion in 2005 to RUB 27 billion in 2006 and RUB 39 billion in 2007. The FCS (including its law enforcement subsidiaries) appears to be adequately structured and funded, and it has sufficient operational independence and autonomy. The FCS has a staff of 1 882 persons at its headquarters and 63 797 persons in regional departments (2005: 57 000 / 2006: 63 600). 5 823 of these work in law enforcement departments, around 2 000 in economic crime related departments, of which again 400 persons could work on ML/TF cases. Taking into consideration the growing number of cases, the evaluators believe that more specialised staff should be hired to deal with ML and TF through cross-border transportation of currency.

292. Customs officials are bound by secrecy provisions, breach of which is punishable. For breach of commercial, tax and bank secrecy the punishment is imprisonment for up to ten years (CC article 183). For breach of state secrecy, the punishment is imprisonment for up to seven years (CC article 283). Selection of staff is based on criteria listed in an internal order[73], which delineates the qualifications for assignments.

Training (Recommendation 30)

293. Training and guidance is provided to all FCS bodies, including general guidance on countering smuggling[74]. The publication "Counteracting Customs Crimes and Money Laundering"(Moscow, Law and Justice Publishers, 2000) has been used to draft methodological recommendations sent to all FCS units[75]. In addition (after the on-site missions) in February 2008, the FCS issued an official letter to all heads of operational FCS divisions requiring them to focus more closely on issues relating to cross-border cash and bearer negotiable instrument movements[76], thereby

---

[72] Gostechcomission Order no. 282 of 30.08.2002 on technical safeguarding of information, FCS Orders of 19.09.2006 on the concept of information security measures for FCS, no. 1062 of 30.10.2006 on information security measures in the process of co-operation with other bodies, no. 168 of 06.02.2007 on access to FCS joint information database and others.

[73] Federal Law of 21.07.1997 no. 114-FZ On the Service for Customs Bodies of the Russian Federation, Order of 02.04.2001 no. 327 On the approved list of senior, middle and junior positions of customs bodies.

[74] The Investigation of Smuggling (Moscow, Jurist Publishers, 1999), The Investigation of Smuggling in Trade and Avoidance of Customs Fees under the new Customs Code (Moscow, 2005), Legal and Criminality Aspects of the Prevention Smuggling in Trade and Avoidance of Customs Fees (Moscow, RIO RTA, 2006.

[75] "Methodical recommendations on the procedure establishing involvement in ML/TF of the persons related to smuggling criminal cases" (no. 01-16/48817 of 19.12.2007); "Methodical recommendations on classification of customs administrative offences and on administrative investigation" (no. 01-06/16066 of 28.04.2007).

[76] FCS official letter no. 07-224/1053, of 20.02.2008.

pro-actively confirming one of the findings of the evaluation team (for which the authorities should be commended).

Statistics and effectiveness

294. Russia keeps statistics on the number and amount of cross border declarations made (incoming and outgoing). For the period January to September 2007, Russia received 939 356 forms from incoming passengers and 1 066 084 forms of outgoing travellers. Every passenger entering or leaving Russia has to complete such a form, and the form contains 12 categories of merchandise that need to be reported (including cash and bearer negotiable instruments). It is not clear to the evaluation team if these numbers concern all declarations or only those that refer to cash or bearer negotiable instruments. The authorities keep statistics on the number of cases related to cash smuggling (2006: 474 and 2007: 460) and investigations related to administrative offences (2006: 3 635 and 2007: 7 189). However, these cases may relate to other crimes than ML or TF. In absence of any ML/TF related figures, it is difficult to assess the effectiveness of the system for ML and TF.

295. There seems to be a high level of corruption within the FCS that generally impedes on the effectiveness of the system. Nevertheless, the authorities have taken steps in order to prevent corruption, such as the periodic transfer of employees, training, special anti-corruption programmes and internal control procedures. The rise in budget per employee (from RUB 329 000 in 2005 to RUB 612 000 in 2007), although not completely dedicated to salary increases, also lowers the risk of corruption within this service.

2.7.2 Recommendations and Comments

296. Overall, the evaluation team does not regard the current system for detecting and preventing cross border movements of currency to be comprehensive or effective in the fight against ML and TF. Considering that, according to the authorities, some popular money laundering methods in Russia involve the movement of cash to and from Russia, the evaluation team urges the authorities to act upon its own typologies findings and implement all elements of an effective system to deter illegal cross border movements of currency.

297. The FCS indicated that it is well staffed, while recognising that the increasing number of cases puts a burden on the service. The evaluation team believes that current staffing levels should be increased to keep up with the growing workload, also in order to increase the effectiveness.

298. Customs seems to be affected by corruption, which impacts on the effectiveness of the FCS and its AML/CTF duties. The evaluators applaud the measures taken so far to prevent corruption and encourage the FCS to continue fighting corruption.

299. Russia is a cash-oriented economy, and the central authorities are well aware of the fact that cross border currency movements are important means to launder money and finance terrorism. Nevertheless, the evaluation team found that the Customs staff in the majority of the regions that were visited are not convinced that cash smuggling is an issue that should be targeted for AML/CFT reasons. Only one Customs border regional division reported such cases (Kaliningrad), while all other regions (Caucasus, Central, Ural and Far East) denied the existence of cash smuggling in their regions. Nevertheless, the evaluation team was provided with examples of related criminal cases investigated by other law enforcement agencies (MIA, FSB) in these regions. The evaluation team urges the authorities to immediately commence an awareness raising campaign, for all levels of staff in all regions. In addition, the authorities should ensure that customs and law enforcement co-operate in all regions and are aware of each others' cases, especially relating to the fight against alternative remittance systems (see section 3.11 of this report).

300. The legal provisions for defining which bearer negotiable instruments are covered by the declaration system can be found in a variety of laws (CCRL, Civil Code), and during the course of the on-site visit the evaluation team was presented with many contradictory explanations. It was illustrative that even the responsible staff at Customs (region and headquarters) were not aware of the exact obligations for travellers. Also the fact that the Russian and English versions of the Customs declaration forms refer to different bearer negotiable instruments does not add to the clarity of the law. Russia should also ensure that sending cash or bearer negotiable instruments through containerised cargo is covered in law and practice.

301. The FCS should have the legal authority to restrain currency in case of suspicions of ML if the money is declared. The FCS should take into consideration a system to use reports on currency declaration in order to identify and target money launderers and terrorists.

302. The administrative penalties for false or non declarations should be raised considerably. Taking into account the low chances of detection, the fines are not considered to be dissuasive or effective. The possible confiscation of the cash is not dissuasive, in particular not in cases where the cash or bearer negotiable instruments are smuggled on behalf of a third person who actually owns the money.

2.7.3 Compliance with Special Recommendation IX

	Rating	Summary of factors relevant to s.2.7 underlying overall rating
SR.IX	**NC**	• No clear power to stop or restrain declared cash or bearer negotiable instruments in case of a suspicion of money laundering. • Customs declaration forms are not in line with the requirements set in the law. • Customs authorities do not keep all required data relating to ML/TF. • There is inadequate co-ordination among relevant competent authorities on cross border cash movement (effectiveness). • The administrative fines available for false or non-declarations are not dissuasive and not effective. • Customs staff seem not to be aware that the system can be used for AML/CFT purposes (effectiveness). • Insufficient number of dedicated AML/CFT staff at the borders. • Corruption seems to affect the effectiveness of the system. • Failures under Special Recommendation III have a negative impact. • Sending cash through containerised cargo is not covered and implementation through general provisions was not demonstrated. • The authorities could not demonstrate the effectiveness of the system.

3. PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

3.1 Risk of money laundering or terrorist financing

303. Russia has decided to apply its AML/CFT framework equally to all financial institutions, irrespective of the level of risk. However, some of the designated FIs may, in certain circumstances, determine the degree of risk attached to particular types of customers, business relationships, transactions or products, and apply simplified or enhanced due diligence rules. The detailed rules concerning enhanced and simplified due diligence are described and assessed in section 3.2 of this report. Overall, there is a combination of prescriptive rules for simplified due diligence and less prescriptive guidance for enhanced due diligence, which allows certain FIs a degree of latitude in determining the level of risk of a customer or transaction.

304. The supervisory regime is not fully risk-based, with a large number of visits planned around a periodic visit programme. However, certain supervisors use an element of risk in planning both scheduled and unscheduled visits, using factors such as information obtained from numbers of STRs and from other alerts which might generate a need to visit. In particular, the regional supervisory authorities spoken to by the evaluation team did not consider that any of the regions were subject to specific financial crime risks. This is surprising, given the size and diversity of the country, and did not accord with the views of some of the financial institutions spoken to, who were able to identify regional variations in ML/FT risks.

305. Russia has certain entities (Payment acceptance [приём платежей in Russian] and money transfer service providers, see section 1.3) that provide money transfer services for payment of telecommunication services, rents and utility services (see section 1). The evaluation team was not given the opportunity to meet with any of these institutions during the on-site visits, and thus the precise nature of their activities and the effectiveness of the measures they are taking could not be assessed.

306. The evaluation team met with a leasing company which appeared to only carry out business-to-business operational leasing and thus was not within the FATF definition of financial leasing. The evaluation team was not, therefore, able to discuss issues relevant to effectiveness with this type of financial institution.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)

3.2.1 Description and Analysis

Legal framework

307. The legal framework for customer due diligence is set out in a variety of legal documents. Except for the AML/CFT Law, all these constitute other enforceable means. See section 1.1 for a description of the hierarchy of laws, regulations and other enforceable means.

308. Only the AML/CFT Law[77] qualifies as "law or regulation", while all other documents qualify as "other enforceable means". As with all Mutual Evaluations, this distinction is important to bear in mind when assessing those Recommendations that must be (partially or wholly) implemented through law or regulation. The AML/CFT Law was issued by Parliament and applies to all sectors that are designated. The other documents apply to different sectors.

309. The following other documents (all other enforceable means) constitute the legal framework for customer due diligence: Decisions 983R[78] and 6[79] (both issued by the Government and apply to all FIs except for CIs), Order 104[80] (issued by Rosfinmonitoring and applies to all FIs except for CIs),

[77] Federal Law of 07.08.2001 no. 115-FZ On Combating Legalisation (Laundering) of Proceeds from Crime and Financing of Terrorism as revised by Federal Law of 12.04.2007 no. 51-F.

[78] Government Decision of 17.07.2002 no. 983-r On Approval of Recommendations on Development of Internal Control Rules for Combating Legalisation (laundering) of the Proceeds from Crime and financing of terrorism by Organisations involved in operations with monetary funds and other property.

[79] Government Decision of 07.01.2003 no. 6 "On the procedure for the approval of the rules for internal control in organisations performing operations with monetary funds or other property".

[80] FMC Order of 11.08.2003 no. 104 "On Approval of Recommendations on Specific Provisions of Internal Control Rules Developed by Organisations Performing Transactions with Monetary Funds or other Property for Combating the Legalisation (laundering) of Proceeds from Crime and Financing of Terrorism".

Regulation 262-P[81], Operative Direction 7-T[82], Instruction 28-I[83], Letters 115-T[84] and 92-T[85] (all issued by the BoR and apply to CIs) and Order 613/R[86] (issued by the FSFM and applies to securities).

310. References to "financial institutions" in this section apply equally to credit institutions, securities, insurance, foreign exchange, MVT services and all other financial sectors (see article 5 AML/CFT Law) except for DNFBPs. The requirements that apply to all financial sectors set out in Law 115-FZ ("the AML/CFT Law") are only mentioned once in the first section for each criterion, and are not repeated in subsequent sections. Additional relevant requirements affecting the banking and other sectors are set out only where the criteria can be met by other enforceable means.

Recommendation 5 (Customer identification and due diligence)

Anonymous accounts

Credit institutions

311. Credit institutions are explicitly prohibited from opening anonymous accounts, which is defined as opening an account without providing the documents required for identification to the institution opening the account (AML/CFT Law, article 7 clause 1.5). There is no specific provision that prohibits banks from maintaining existing accounts under fictitious names. Numbered accounts exist in Russia and Central Bank Letter 7-T (which is treated as other enforceable means) reminds credit institutions of their obligations under the AML/CFT Law when opening and managing numbered accounts, but there are no specific requirements in law or regulation. The financial institutions spoken to by the evaluation team reported that they did not open or maintain anonymous or numbered accounts and the Russian authorities have stated that, in their view, the requirement to identify account holders automatically prohibits credit institutions from maintaining accounts in fictitious names. However, there is no specific prohibition in law or regulation.

When establishing a business relationship

AML/CFT Law

312. The basic rule that applies to all designated entities under the AML/CFT Law is that all customers on whose behalf an organisation is "performing operations with monetary funds" must be identified. This is a broad term which covers the establishment of business relationships. FIs are required to collect the following data: surname, name, patronymic name, date and place of birth, citizenship, ID document data, migration card data, resident's permit data, address, tax identification number. Legal persons are required to supply the FI with name, tax identification number, state registration number, address and place of state registration (AML/CFT Law, article 7, clause 1, sub 1 to 5). In certain cases, exemptions to this rule have been established. These exemptions are discussed below in other subsections.

---

81 BoR Regulation of 19.08.2004 no. 262-P On the Identification by Credit Institutions of Clients and Beneficiaries for the Purposes of Combating Legalisation (Laundering) of Proceeds from Crime and Financing of Terrorism.

82 BoR Operative Direction of 20.01.2003 no. 7-T On the Implementation of the Federal Law On Combating Legalisation (Laundering) of Proceeds from Crime and Financing of Terrorism.

83 BoR Instruction (14.09.2006) no. 28-I On opening and closing bank accounts and accounts for deposit (deposit accounts).

84 BoR Letter of 30.08.2006 no. 115-T On the Implementation of the Federal Law On Combating Legalisation (Laundering) of Proceeds from Crime and Financing of Terrorism as regards the identification of customers serviced using remote banking service technologies (including Internet banking).

85 Letter of the BoR no. 92-T of 30.06.2005 "On Organising the Management of Legal Risk and Risk of Losing Business Reputation at Credit Organisations and in Banking Groups".

86 FSFM Order no. 613/R of 03.06.2002 adopts methodological recommendations on the realisation by professional players in the securities market of the requirements of the AML/CFT Law".

When carrying out an occasional transaction

AML/CFT Law

313. The rules that apply to the establishment of a business relationship also apply to occasional transactions. However, if the transaction does not exceed the threshold of RUB 30 000 and falls within the following specific categories, no identification and verification of customer and beneficiary is required. The exemptions are (AML/CFT Law, article 7, clause 1.1):

- "Related to settlements with budgets of all levels of the budget system of Russia (including federal, regional and local taxes and duties, as well as fines provided for by Russian legislation on taxes and duties).
- Related to payment for services rendered by budget institutions under the management of federal executive bodies, executive bodies of the Federal Subjects and bodies of local self-government.
- Related to payment for flats, local services, payment for safeguarding flats and instalment of alarm systems, as well as payment for communications services.
- Related to payment of contributions by members of orchid, garden, non-commercial associations of citizens living in summer houses, garage-construction co-operatives. Payments for paid auto placements.
- Related to payments for alimony."

314. Foreign exchange transactions are likewise exempted from any identification or verification of the customer and / or the beneficiary, if the amount does not exceed a threshold of RUB 15 000. The exception to this exemption would be any suspicion of ML or TF (AML/CFT Law, article 7, clause 1.2).

315. It is not entirely clear what risk analysis Russia has carried out in order to choose these specific categories for relaxing the criteria. However the Russian authorities explained that when drafting the set of operations which do not require CDD, the social nature of the operation and their limited size were taken into account. The evaluation team does not consider this to be an adequate risk assessment.

When there is a suspicion of money laundering

316. Transactions below the threshold of RUB 30 000 falling within the exempted categories described above never have to be identified and verified, regardless of whether there is a suspicion of ML or TF. In all other cases, transactions have to be identified in case there is a suspicion of ML/TF.

When carrying out wire transfers

317. Wire transfers can only be executed by credit institutions, postal organisations and non-bank credit institutions. The CDD rules that apply for business relationships and occasional transactions, also apply for wire transfers, whether from an account or as a money transfer. Russia Post (one of the money transfer operators) has set up internal guidelines[87] to ensure compliance with CDD rules.

[87] Russia Post Order no. 81-P of 13.03.2007 "On adoption of the forms for post transfers for monetary funds".

When there are doubts about the veracity/adequacy of previously obtained customer identification data

AML/CFT Law

318. There is a general requirement for FIs to "regularly" update information on customers (AML/CFT Law, article 7, clause 1, sub 3). No further clarification is given, and the financial institutions spoken to by the evaluation team saw this as a requirement to update on a periodic basis (usually annually). There is, therefore, no explicit requirement in law or regulation to carry out CDD in these circumstances.

Required CDD measures

Natural persons

319. To identify natural persons, FIs are required to collect the following data: surname, name, patronymic name, date and place of birth, citizenship, ID document data, migration card data, resident's permit data, address, and tax identification number. In practice, FIs rely on information contained in passports for domestic customers. In order to mitigate the risk of the use of fake passports and increase the effectiveness of the verification procedures, government agencies are required to supply reporting entities with information on void or stolen passports or passport forms. In order to implement this provision the MIA compiles a list of fake and lost passport numbers, which it sends to the supervisory authorities, who then pass this on to supervised institutions. A database of void passports is contained on the website of the Federal Migration Service. For overseas customers, FIs rely on passports and the data contained in migration cards (AML/CFT Law article 7, clause 1, sub 1 and article 9, item 5).

Legal persons

AML/CFT Law

320. If the customer is a legal entity, the AML/CFT Law prescribes that both the customer and the legal or natural person representing a customer have to be identified, as if both were establishing a business relationship or performing an occasional transaction. This means that for legal persons, information concerning the customer's name, taxpayer's identification number, state registration number, place of state registration and address will be collected. Proof of incorporation is established by the collection of the state registration number, which links in to the Unified Central Registration System (USRLE) to which all FIs have access. In addition, the FI needs to establish on what basis the person acting on behalf of the legal entity is authorised to do so (*e.g.* via a power of attorney, contract, law, proxy etc.). In order to increase the effectiveness of implementation, the FTS issued an order[88] that sets out the form of the request to be used by the bank, as well as a 5-day response-time for the FTS authorities to answer the request of the bank. In order to mitigate the risk posed by "one-day front companies" the FTS also provides credit institutions with a database[89] of so-called mass-registration addresses[90] (AML/CFT Law, article 7, clause 1, sub 4).

[88] No CAE-3-09/325 of 15.07.2005) on provision of information from the State register of legal persons to CIs at their request.

[89] FTS Letter No 09-1-03/3103 (16.06.2006).

[90] A mass registration address is a single address, to which many companies are registered. This is usually an indicator of the fictitious nature of the companies registered.

Legal arrangements

AML/CFT Law

321. The concept of legal arrangement is unknown in the Russian legal system, therefore, the AML/CFT Law and any other legal document is silent on this issue. The Russian authorities did not indicate what FIs would be required to do if a legal arrangement from abroad wants to establish a business relationship or perform an occasional transaction. In practice, the financial institutions spoken to had no experience of dealing with legal arrangements.

Authorised representatives

AML/CFT Law

322. The law does not specifically express that FIs should determine whether a customer is acting on behalf of another person. However, if this information becomes available, the law does indicate that the person on whose behalf an operation with monetary funds is carried out has to be identified, and that migration card and resident permit data have to be collected, as well as the tax identification number and the place of residence. The law states that a beneficiary must be identified. This provision appears to cover persons on whose behalf the customer acts. However, this provision only requires identification of the beneficiary and not specifically checking whether the person is authorised to act on behalf of the customer (AML/CFT Law, article 7, clause 1, sub 2 and 4).

Beneficial owner

AML/CFT Law

323. The English translation of the AML/CFT Law refers to the requirement for identifying "beneficiaries". This does not appear, in theory or in practice, to require an FI to establish who the ultimate natural persons who own or exercise control over a legal person are. For credit institutions only, Regulation 262-P and Letter 92-T (even though these documents are other enforceable means) provide some guidance. In Regulation 262-P "beneficiary" is defined as "the person in whose favour the customer acts, in particular on the basis of an agency contract, contracts of agency, agency and trustee management for performing banking operations and other deals" (Chapter 1.2), and further in Letter 92-T, as "the persons for whose benefit customers act" (Chapter 2.1.1). Both do not fully match the FATF definition of beneficial owner.

324. The evaluation team was given conflicting interpretations of the provisions relating to the need to identify "beneficiaries". The majority of FIs spoken to interpreted the requirement as imposing the need to identify those acting on behalf of another person.

Ownership and control structure

Credit institutions

325. Regulation 262-P requires credit institutions to take certain steps to identify legal entities, including obtaining information on the structure and composition of the administrative body (Appendix 2).

Other financial institutions

326. Ordinance 983R obliges FIs to pay special attention to the composition of the founding members, structure of managing bodies of the legal entity and their powers, the amount of registered and paid authorised (share) capital when identifying a legal person. This does not amount to a requirement to understand the ownership and control structure of the customer (Ordinance 983R articles 9 and 10).

Natural persons that ultimately own or control the customer

AML Law

327. Beyond the requirement to identify "beneficiaries", there is no formal requirement in the AML/CFT Law to determine who the natural persons are that ultimately own or control the customer.

328. The financial institutions spoken to by the evaluation team did not consistently appear to understand the concept of beneficial ownership, and did not always appear to trace ownership of legal entities down to the ultimate natural person, especially in the case of overseas customers. In addition, they did not always link the need to do this with a requirement in the AML/CFT Law.

Purpose of the business relationship

AML/CFT Law

329. The AML/CFT Law obliges FIs to record information on "the type of operation and grounds for performance thereof" (article 7, clause 1, sub 4). This appears to only apply to operations which are subject to obligatory control (i.e. mandatory reporting). This is a transaction-related requirement that will enable the FI to build an understanding of the purpose of the business relationship. Nevertheless, the requirement does not meet the FATF standard, which is focussed on ascertaining this information at the start of a business relationship. The related requirement to collect data on a customer's activity may provide some additional information, but is insufficiently specific.

Credit institutions

330. For credit institutions, Regulation 262-P includes the requirement that credit institutions gather data and documents constituting grounds for performing banking operations and other transactions (Regulation 262-P, item 2.1). However, one credit institution spoken to by the evaluation team did not feel that this requirement obliged them to obtain information on the purpose of why the customer was opening an account. Separate requirements on establishing the purpose of the business relationship have been established for non-resident customers of CIs (see below on enhanced due diligence).

Other financial institutions

331. Decision 983R effectively repeats the provision in the AML/CFT Law, by making a recommendation that FIs document the "type of operation and the grounds for the accomplishment thereof". Again, this does not amount to a specific requirement to ascertain the purpose and intended nature of the business relationship.

Ongoing due diligence

AML/CFT Law

332. There is no duty for FIs to conduct ongoing due diligence on business relationships. However, there is a requirement in the AML/CFT Law that FIs have to "regularly" update information on customers and beneficiaries. "Regularly" is not further defined, and does not necessarily mean that data or information collected under the CDD process will be updated (AML/CFT Law article 7, clause 1.3).

Credit institutions

333. Regulation 262-P requires CIs to update identification information "as changes are introduced" but "at least once per year" for higher risk customers and "at least once in three years" in

other cases. The CIs spoken to by the evaluation team tended to adhere to the time limits. Additional measures are set out in Letter 99-T for detecting unusual transactions.

Other financial institutions

334. Decision 983R recommends that FIs update identification and verification information at least once a year (article 11). There is a general requirement that the relevant information be documented (article 6 d). Additional measures are set out for detecting unusual transactions.

335. Order 104 recommends that FIs "update periodically" the information on identification received from customers. This is defined as at least once a year for high risk customers and at least once every 3 years for other customers (article 2.5). In addition, article 2.2.1 requires that an FI "identify and study its client during the completion of operations in accordance with the legislation of Russia". This is not further defined.

336. For securities institutions, information about a customer should be updated at least once a year (Order 613/R article 5.1.4).

337. CIs and FIs spoken to by the evaluation team recognised the need to update CDD information on a defined periodic basis, but did not otherwise appear to conduct ongoing CDD except in circumstances which gave rise to the need to submit an STR.

338. In practice not all FIs are routinely checking source of funds, especially for money transfers submitted through Russia Post.

Customer risk

Enhanced due diligence

AML/CFT Law

339. The basic rule for enhanced CDD is contained in the AML/CFT Law, which stipulates that identification requirements may vary according to the level of risk for a customer or transaction. While this basic rule applies to all FIs, it is assumed that only credit institutions may apply it, since only this sector has additional specific rules (AML/CFT Law article 7 clause 2).

Credit institutions

340. Regulation 262-P for the credit institution sector sets very detailed rules for enhanced CDD in cases deemed to be higher risk. The rules are minimum requirements, and the regulation explicitly states that other operations may also be of a high risk nature. Credit institutions do not necessarily have to perform enhanced CDD if a customer or transaction matches any of the criteria. The criteria solely require a credit institution to estimate the degree of risk. Examples of criteria are transactions involving pawnshops, gaming entities, antiques, furniture, cars, precious metals and stones, real estate, transactions of customers that have a history of smurfing, internet banking transactions and transactions with jurisdictions and their residents that have not implemented the FATF Recommendations (Regulation 262-P, article 2.9 – 2.9.13). There is, however, no additional guidance on what additional CDD measures a CI should take. In practice, the CIs spoken to by the evaluation team added their own criteria to those in the Regulation. The only obvious effect of having a customer in a high risk category is the need to update CDD information at least once a year, and a general requirement to devote special attention to (quote) "deals of an increased degree (level) of risk in monetary funds or other property closed by the customer" (Regulation 262-P, article 2.10). For credit institutions, enhanced identification requirements have been in force since 30 October 2007 in relation to non-resident customers (non-Russian taxpayers)[91]. Prior to establishing a business relationship with

[91] BoR Letter 170-T.

such a customer a credit institution must obtain a range of additional information. CIs are only permitted to open accounts or commence business relationships with such customers with the permission of the top manager of the CI or an official specifically designated by him. As these provisions only recently came into force, the evaluation team was not able to assess their effectiveness.

Other financial institutions

341. For other financial institutions, Rosfinmonitoring Order 104 also sets out specific criteria for operations that could be considered higher risk. The list contains nine broad criteria that FIs should take into account. This list is non-exhaustive, and FIs may add their own criteria to this list. The main impact of this provision is that information on high risk operations will be collected more frequently (at least once a year) and financial institutions will be required to pay more attention to such operations (article 2.5 and appendix 4).

Simplified due diligence

AML/CFT Law

342. FIs are not allowed to apply reduced or simplified CDD measures, except in specific circumstances. These circumstances are all actually exemptions to the general identification / CDD rules, rather than simplified rules. FIs do not have a choice whether or not to apply the exemptions if they feel that the risk is indeed higher, as the exemptions to the rules are mandatory. Most of these exemptions are already discussed (see occasional transactions).

343. There are no rules with respect to transactions with jurisdictions and their residents that have not implemented the FATF Recommendations. In addition, a suspicion of ML or TF would not lead to an exemption to the simplified CDD rules, except when the simplified CDD is in relation to a foreign exchange transaction below the threshold of RUB 15 000.

Credit institutions

344. In addition to these rules, state authorities (on all levels) do not need to be identified (Regulation 262-P, item 1.6). Credit institutions are permitted to apply simplified customer identification in circumstances involving the transfer of monetary funds by a natural person or for certain foreign currency transactions for natural persons. This relaxation of the normal customer identification rules is not permitted where there is a suspicion of ML or TF.

345. The enhanced CDD rules are of a lower force than the AML/CFT Law that provides for the exemptions. Overall, the rules determining mandatory exemptions and possible enhanced measures for CDD seem to be somewhat prescriptive and not based on risk assessments carried out by FIs.

Timing of verification

AML/CFT Law

346. The AML/CFT Law is silent with respect to the timing of verification, leaving some uncertainty for FIs. Except for credit institutions, there are no specific additional requirements that could assist FIs.

Credit institutions

347. For credit institutions, Regulation 262-P states that identification may take place within seven working days after the business relationship has commenced or an occasional transaction has taken place if identification and verification is not immediately possible. There are no special requirements, such as compulsory risk management procedures, for credit institutions to postpone

completion of identification or verification. In addition, the use of this relaxation of the identification requirement is not limited to cases where it is essential not to interrupt the normal conduct of business, nor does the requirement to manage ML/TF risks play any role (Regulation 262-P, article 2.8). In practice, most CIs spoken to by the evaluation team appear to complete verification of identification before opening accounts.

Failure to complete CDD

AML/CFT Law

348. The AML/CFT Law requires FIs to refuse to carry out a transaction, except for incoming funds, if the necessary identification information is not presented. This relates solely to the identification requirement, and there are no further rules dealing with failure to obtain details of the purpose and intended nature of the business relationship (article 7.11). This article puts in place an obligation for all FIs, but since it relates to wire transfers (as defined by FATF Special Recommendation VII), only CIs and Russia Post are affected by it.

Credit institutions

349. The AML/CFT Law allows credit institutions to refuse to open an account when a person or legal entity fails to submit identity documents, if invalid documents are submitted or if the customer is linked to terrorist activity (article 7 clause 5.2). Accounts may not be opened for shell banks, for anonymous owners, or for customers (or their representatives) who do not personally present themselves. CIs are only permitted to reject a transaction in the absence of the required documentation or if the customer is linked to terrorist activity. However, this does not extend to the receipt of incoming funds, which appears to be a potentially significant omission. In these circumstances CIs are required to submit an STR (article 7 clause 13). Termination of a business relationship is only allowed in certain limited circumstances.

350. There are no specific rules covering non-CIs, which appears to be an important omission.

351. FIs spoken to by the evaluation team indicated some frustration that they are not able to close accounts on the basis of AML/CFT risk (except for non-face-to-face customers), and one indicated that other means, such as increasing charges, would be used to terminate business if suspicions arose. Similarly, an FI cannot refuse to open an account on the basis of AML/CFT risk, and FIs can resort to asking for increasing amounts of documentation from the customer in order to avoid opening the account. The evaluation team was told that one of the banking associations is lobbying the government to change the circumstances in which a CI could refuse to open an account or close an account.

Treatment of existing customers

AML/CFT Law

352. The AML/CFT Law obliges FIs to “regularly update” customers’ information, which refers to the information collected at the start of a business relationship (AML/CFT Law article 7 clause 13).

Credit institutions

353. Credit institutions are obliged to update customer identification information at least once every three years. When regulation 262-P (item 4.2) entered into force (August 19, 2004), CIs were required to implement all CDD requirements in relation to all customers "that are making use of their services" within a year. The Russian authorities consider this to require that CDD be extended to all existing customers. The evaluation team was not given information on how effectively this requirement has been adhered to.

Other financial institutions

354. Decision 983R requires non-CI FIs to update identification information every year (article 11).

Effectiveness

355. Russia has certain of the key elements relating to customer due diligence clearly set out in law or regulation, with some of the elements covered by other enforceable means. However, the overall picture is somewhat fragmented, with certain elements, such as enhanced and simplified due diligence, apparently inconsistent. In addition, some of the factors do not apply to all FIs, with the most comprehensive elements applying to credit institutions. The authorities make use of ad hoc letters and decisions to clarify certain issues, but there is some uncertainty amongst supervised institutions about what measures are strictly required.

356. Some FIs apply their own, higher standards, especially those FIs that are part of a larger group. Whilst this arguably increases effectiveness, the steps they are taking are as a result of individual group policies as opposed to an interpretation of the measures set out in the existing legislation and guidance.

357. Particular areas of concern involve the uneven approach amongst FIs towards the concept of identifying the ultimate natural persons who own or control the company and the inconsistent requirements to perform ongoing due diligence other than on a time limited basis. In addition, few institutions are establishing the purpose and intended nature of the business relationship and are concentrating on transaction-related criteria which are necessary for establishing when mandatory control reports should be submitted.

358. FIs spoken to by the evaluation team expressed a degree of frustration over the fairly prescriptive rules applying to situations where they can refuse to open an account or carry out a transaction, as well as when they can close accounts (except for non-face-to-face relationships). At present, FIs use other means (such as increasing charges or requesting additional documentation) to manage situations where they perceive the ML/FT risk as being high.

359. Further development of the guidance for determining risk and especially the steps to take to mitigate risk, rather than relying solely on the requirement to submit STRs, would doubtless enhance the effectiveness of the CDD requirements.

360. The existence of "one day companies" is a further matter of concern and one which is shared by the Russian authorities. Steps to tighten the measures for identifying such companies would close a potential gap in the system, and make the financial sector less vulnerable to exploitation.

Other enforceable means (effectiveness)

361. Some of the provisions of BoR Regulation 262-P (which is treated as other enforceable means) partially cover the gaps in law or regulation for credit institutions, specifically where there are doubts about the veracity or adequacy of identification information previously obtained, and in relation to ascertaining whether a client is acting on behalf of another. These arguably enhance the effectiveness of the system.

Recommendation 6 (Politically exposed persons)

362. Until January 2008[92], the Russian authorities had not implemented any specific requirements in relation to politically exposed persons (PEPs). This was a surprising omission in a country which, in its NASP, identified corruption (albeit domestic corruption) and financial activity by foreign nationals

[92] The AML/CFT Law was amended in November, but entered into force on 15 January 2008.

as a matter of concern. In addition, the President acknowledged the problem of corruption in his State of the Nation Address in 2006 (see section 1 for more information on corruption).

363. In November 2007 the State Duma and Federation Council approved amendments to the AML/CFT Law which specifically deal with PEPs. The provisions did not come into effect until 15 January 2008, and thus the evaluation team was unable to assess their effectiveness.

364. The new provisions oblige institutions to take steps to identify customers who are "foreign public persons (FPP)". This term is not defined in the Law. Before 15 January 2008, guidance was issued to all FIs advising them about the applicability in this case of the definition of FPP as contained in the UN Convention against Corruption, which was ratified by Russia and is considered to be a part of the Russian legal system. Such guidance was posted on the website of Rosfinmonitoring, and includes "any person holding a legislative, executive administrative or judicial office". The BoR has issued a letter informing CIs of this definition of FPPs[93]. The Association of Russian Banks also issued guidance on the definition of FPPs, but this private sector guidance document has not been provided in English, and thus could not be verified. However, as stated on the Rosfinmonitoring website, the definition only extends to FPPs "holding" an office or "exercising" a public function. The FATF definition extends to those "who are or *have been*" entrusted with public functions. In addition, the requirement does not extend to beneficial ownership. Business relations with foreign public persons can only be established with the written approval of the head of the organisation (article 7, clause 1.3, item 2). However, this provision appears only to extend to situations where an FI is establishing a business relationship, and thus does not extend to existing customers subsequently found to be PEPs.

365. Institutions are required to establish "the source of the monetary funds or other assets of foreign public persons" (article 7, clause 1.3 item 4 and 5). In the absence of additional guidance, it is not clear whether the intention of this provision is to include an analysis of the source of the subject's wealth.

366. Information on foreign public persons is required to be updated "on a permanent basis" and institutions are required to pay higher attention to operations performed by or on behalf of such persons, their spouses or close relatives (article 7, clause 1.4 and 5). The Russian authorities consider that the requirement to "pay higher attention to transactions" is intended to provide for the scrutiny of transactions of PEPs. As the provisions were not in effect at the time of the on-site visits, and in the absence of any further guidance, it is not possible to confirm what steps institutions are required to take in order to comply with this part of the Law.

Additional elements

367. The above requirements have not been extended to include domestic PEPs.

368. Russia signed and ratified the United Nations Convention against Corruption on 10 December 2003 and 8 March 2006 respectively.

Recommendation 7 (Correspondent banking and similar relationships)

Credit institutions

369. Correspondent relationships with other banks are governed by the AML/CFT Law, Banking Law, Regulation 262-P and Direction N 1317-U. Correspondent relationships are only allowed with banks that are established in a jurisdiction with a permanent supervisory body, and the respondent bank itself should only have correspondent relationships with such banks. Russian banks are required to treat their correspondent relations as normal non-resident customers and ask for all the documentation that legal entities have to supply to open an account in Russia (see the description of

[93] BoR Letter, NO. 8-T (18.01.2008).

Recommendation 5 earlier in this Section). Even though this information may allow CIs to generally understand the nature of the respondent's business there is no specific requirement for Russian banks to determine from publicly available information the reputation of the institution and the quality of supervision. The Russian authorities consider that the list of offshore states and territories published by the BoR is an indicator of the quality of supervision. Russian banks are also not required to ascertain whether the respondent bank has been subject to a money laundering or financing of terrorism investigation or regulatory action. By contrast, Russian banks are required to request information on the respondent's AML/CFT system, but there is no specific requirement to ascertain whether they are adequate and effective. A special regime has been established for correspondent relationships with banks from offshore jurisdictions. In those cases, the respondent bank is treated as a high risk customer[94]. In addition, correspondent relationships with banks of many other jurisdictions[95] are only allowed if the respondent bank has a minimum capital of EUR 100 Million (AML/CFT Law, article 7, clause 5 and 5.1, Banking Law, article 28, Regulation 262-P, item 3.4, Direction N 1317-U).

370. Correspondent relationships have to be approved by the head of the bank, or by one of the employees authorised to do so by the head of the bank. The respective AML/CFT responsibilities of each institution do not need to be documented, but the Russian authorities informed the evaluation team that they consider that the responsibilities of the Russian banks are clearly documented in the AML/CFT Law. While this might be true in principle, this would mean that the respondent bank would need to understand the Russian legal framework, with possible misinterpretations. Also, it would do nothing to solve practical problems that are not foreseen in the law.

371. The Russian authorities stated that Russian banks are not allowed to provide payable-through accounts, because BoR Instruction 28-I does not specifically provide the power for them to do so. The Russian regulatory system for the financial sector is rather prescriptive in terms of the types of bank accounts that may be opened. BoR Instruction 28-I not only sets out all of the possible types of accounts, but goes into detail as to the procedures for opening each individual type of account. The authorities consider that the opening of a payable-through account would be considered a breach of this Instruction and lead to a sanction for the credit institution which has opened such an account. It is not clear whether this provision has ever been used.

Effectiveness

372. Although a general framework exists in the AML/CFT Law and BoR provisions, there are notable gaps in relation to what steps a Russian bank should take in order to ascertain the effectiveness of the AML/CFT controls of a respondent bank, and in relation to demonstrating the understanding of the responsibilities of the respective institutions. Whilst the risk of reputational damage and economic risk factors motivate most CIs to take steps to investigate those institutions with whom they establish correspondent relationships, the current requirements do not set out a complete set of steps to be taken to mitigate the risks of dealing with correspondent relationships. One of the larger internationally orientated Russian banks spoken to was not aware of the special regime for dealing with correspondent relationships with banks from offshore jurisdictions. In practice, it appears that payable through accounts do not exist in Russia.

[94] Cyprus; Guernsey (including Sark); Hong Kong, China; Ireland (Dublin and Shannon); Isle of Man; Jersey; Luxembourg; Malta; Singapore and Switzerland.

[95] Andorra; Anguilla; Antigua and Barbuda; Aruba; Bahamas; Barbados; Bahrain; Belize; Bermuda; British Virgin Islands; Brunei Darussalam; Cayman Islands; Comoros (Anjouan islands); Cook Islands; Costa Rica; Djibouti; Dominica; Gibraltar; Grenada; Lebanon; Liberia; Liechtenstein; Macao, China; Malaysia (Labuan island); Maldives; Marshall Islands; Mauritius; Monaco; Montenegro; Montserrat; Nauru; Netherlands Antilles; Niue; Palau; Portugal (Madeira); Saint Kitts and Nevis; Saint Lucia; Saint Vincent and the Grenadines; Seychelles; Sri Lanka; Tonga; Turks and Caicos Islands; United Arab Emirates; United States (Delaware and Wyoming, Puerto Rico and US Virgin Islands); Vanuatu and Western Samoa.

Recommendation 8 (New payment technologies)

New payment technologies

373. FIs are not specifically required to have policies in place or to take measures that may be needed to prevent the misuse of new payment technologies for ML and TF, except for some requirements relating to internet banking, which apply to credit institutions (see below).

Non-face-to-face customers

374. Requirements for non-face-to-face business relationships or transactions focus almost exclusively on internet banking. For other sectors, the issue is only remotely addressed, for example in relation to internal rules that need to be set up to detect STRs (Order 104, Annex 2, sub items 5 and 9).

375. The AML/CFT Law contains a general requirement that credit institutions should not open accounts for natural persons without the personal presence of the customer or their representative (article 7, clause 5). This effectively precludes the use of remote means for establishing customer identity. However, conversations with financial institutions in the banking and securities sectors revealed an increasing incidence of internet banking and on-line trading.

376. For credit institutions, internet banking is labelled as a high risk type of business that requires risk analysis and possibly enhanced CDD or the filing of an STR. In addition, all those who have the right of signature and all those who have access to the account, have to be treated in a similar manner to the account holder, especially in relation to identification requirements. In order to additionally mitigate risks, the BoR has instructed CIs to include risk-management clauses into all internet (*remote*) banking contracts. Such clauses are to include the right of the CI to terminate a business relationship if unusual operations are carried out through remote banking, especially in relation to all non-resident (non-Russian taxpayer) customers. BoR supervisory staff are instructed to pay special attention to remote banking and describes a detailed inspection procedure of banks providing remote banking services. (Regulation 262-P, item 2.9.11, Instruction 28-I, items 1.7 and 1.8, BoR Letters 44-T, 60-T, 115-T and 170-T).

377. No other measures have been taken and no other (emerging) new payment technologies have been studied to assess possible risks. In addition, there is a complete lack of any substantial measure for any other sector than the banking sector, especially the securities and insurance sector. As the financial sector in Russia continues to grow, this is an area which would benefit from further measures for all FIs.

3.2.2 Recommendations and Comments

378. Russia has a general framework for dealing with customer due diligence, which contains several of the criteria required by the FATF Recommendations. However, this framework contains several important gaps, which should be remedied. The measures for dealing with PEPs are not complete, and should be dealt with as a matter of urgency, and further tightening of the provisions in relation to correspondent banking would ensure a consistent approach. Although the financial sector in Russia is relatively new, proactive steps should be taken to develop requirements to mitigate the effect new technologies might have on the AML/CFT regime. Specific recommendations are as follows:

Recommendation 5

379. In relation to Recommendation 5 Russia should ensure that the following are covered by law or regulation:

- A specific prohibition on maintaining existing accounts under fictitious names.

- A requirement to carry out CDD where there is a suspicion of money laundering, regardless of any exemptions.
- Performance of CDD where there are doubts about the veracity of previously obtained customer identification data.
- A requirement to identify beneficial owners and in particular to establish the ultimate natural owner/controller.
- Requirements for conducting ongoing due diligence.

380. In addition, the following matters should be set out in law, regulation or other enforceable means:

- Requirement for non-CIs to understand the ownership or control structure of a legal person.
- Requirement to ascertain the purpose and intended nature of the business relationship.
- Requirements for the timing of verification of identification.
- Consequences of a failure to conduct CDD.

381. In addition, clarification of the requirements relating to enhanced and simplified due diligence would be beneficial, in particular the exemptions from conducting CDD in situations relating to occasional transactions. This is not consistent with the requirement of the FATF Recommendations, which envisages reduced due diligence in appropriate circumstances. Further guidance to FIs on dealing with legal arrangements from overseas would be helpful.

382. A stronger link in the AML/CFT Law between the need to ascertain whether a customer is acting on behalf of another person and the requirement to collect identification data would provide clarity. Further clarification in the AML/CFT Law on the meaning of the term "beneficiary" and the measures which financial institutions should take to comply with the measures would be helpful.

383. Further guidance to FIs would be beneficial to ensure that legal arrangements are appropriately identified as the financial sector grows and becomes more international.

Recommendation 6

384. As the requirements of the amendment to the AML/CFT Law were not in effect at the time of the on-site visits, and there was some doubt as to whether further guidance would be available from the supervisory authorities, the full scope of the new provisions was difficult to determine. However, it is recommended that further guidance be given as to the requirements for dealing with existing customers who are found to be foreign public persons, establishing the source of wealth and conducting enhanced ongoing due diligence. Also, the measures should extend to beneficial owners. Given the concerns set out in the NASP and the concerns of the President of Russia in relation to the endemic nature of corruption in Russia, the evaluation team would also recommend that Russia consider extending the provisions to include domestic PEPs.

Recommendation 7

385. In relation to Recommendation 7, all of the relevant criteria should be set out in law, regulation or other enforceable means, particularly the need to understand the nature of the respondent bank's business and to ascertain whether the respondent's AML/CFT system is adequate and effective. The requirement to document the respective AML/CFT responsibilities of banks should also be covered, and Russia should consider formalising its requirements in relation to payable-through accounts.

Recommendation 8

386. Russia should review the existing limited requirements (which relate largely to remote banking) and to provide appropriate measures on the basis of that review. This is especially important in a financial sector which is growing rapidly.

3.2.3 Compliance with Recommendations 5 to 8

	Rating	Summary of factors underlying rating
R.5	**PC**	• No specific prohibition on maintaining existing accounts in fictitious names. • No requirement to conduct CDD if suspicion of ML/TF if one of the exemptions of AML/CFT Law article 7 clause 1.1 applies. • No requirement in Law or Regulation for dealing with doubts about veracity. • Lack of clarity and effectiveness in respect of beneficial ownership requirements. • Lack of clarity in relation to ongoing due diligence. • No direct requirement to establish nature and intended purpose of business relationship. • Doubts about clarity and effectiveness of requirements relating to SDD and EDD. • Timing of verification – no measures for non-CIs. • Failure to complete CDD – measures for non-CIs only extend to ID.
R.6	**PC**	• Definition of PEPs does not extend to those who *have been* entrusted with public functions. • No requirement for obtaining approval from senior management for existing customers found to be PEPs. • Lack of clarity relating to establishing source of wealth and enhanced ongoing due diligence. • Beneficial ownership is not covered. • No information on effectiveness.
R.7	**PC**	• No specific requirement to understand nature of respondent's business or determine quality of supervision. • No requirement to ascertain if respondent has been subject of ML/TF investigation. • Nothing specific requiring a judgement on effectiveness of respondent AML/CFT system.
R.8	**PC**	• Requirements for new technologies limited to internet banking. • No requirements for non face-to-face transactions except for CIs.

3.3 Third parties and introduced business (R.9)

3.3.1 Description and Analysis

387. Under the AML/CFT Law all financial institutions are obliged to identify customers. While there is no provision that allows financial institutions to rely on a third party to conduct required identification procedures or to introduce business, there is also no provision prohibiting the use of third parties. Nonetheless, article 5, item 7 of the AML/CFT Law specifically prohibits credit institutions from opening an account for a natural person without the personal presentation of the customer or the customer's representative, thus credit institutions are *de facto* not permitted to rely on third parties to verify the identification of a natural person or to introduce business.

3.3.2 Recommendations and Comments

388. Given the law as written and the evaluation team's determination that financial institutions widely understand and abide by the law that prohibits the use of third parties to verify identity or to introduce business, Recommendation 9 does not appear to apply to the Russian system.

389. As the law does not explicitly prohibit the use of third parties, the evaluation team recommends that Russia amend the AML/CFT Law to state clearly that financial institutions are not permitted to rely on third party verification of identity or introduction of business.

3.3.3 Compliance with Recommendation 9

	Rating	Summary of factors underlying rating
R.9	**N/A**	• This recommendation is not applicable (financial institutions are legally not permitted to rely on intermediaries or third parties).

3.4 Financial institution secrecy or confidentiality (R.4)

3.4.1 Description and Analysis

390. The AML/CFT Law clearly intends to ensure that all relevant secrecy or confidentiality laws do not inhibit or prevent the implementation of the FATF Recommendations. The evaluation team detected no practical obstacles to information access or sharing between reporting institutions and competent authorities, between domestic or international competent authorities (provided the appropriate MOUs and international agreements are in place), or between financial institutions when required for correspondent banking activity or cross-border wire transfers. The evaluation team also noted that supervisory authorities seem to have appropriate access, in practice, to information generally protected by financial secrecy provisions but necessary to carrying out their AML/CFT-related supervisory duties.

391. With the exception of the FISS, all supervisory authorities have the appropriate legal authority to override general financial secrecy provisions[96]. The Insurance Law (article 30, paragraph 5) specifically exempts insurance companies from providing information protected by banking secrecy to their supervisory authorities. The Russian authorities have explained that this exemption was designed to reflect the division of supervisory responsibilities between the FISS (responsible for insurance companies) and the BoR (responsible for supervising credit institutions whose deposits are insured by Russia's Deposit Insurance Agency). The rationale behind the

[96] *BoR*: Law on the BoR, article 57 ("to discharge its functions, the BoR has the right to request and to receive from credit institutions the necessary information on their activity in accordance with the list established by the Board of Directors, and to demand explanations on the received information"). *FSFM*: Securities Markets Law, paragraph 7 of article 44 ("to send orders binding for execution to the issuers and the professional stock market participants, and also to their SROs, and also to demand that they submit documents needed for the settlement of the questions coming under the jurisdiction of the federal executive body"). FSFM Order no. 07-108/pz-n (p.3.4.3 - 3.4.6) ("an inspector may demand from the inspected institution, that it supply any documents needed for purposes of the inspection"). Law on Investment Funds ("compel information, including information, to which access is either limited or restricted in accordance with the Federal Law, the necessary explanations and documents needed to discharge its functions". Government Regulation 317 (article 6.1): ("to request for the supply and receive in the established procedure information necessary for decision-making on matters within the jurisdiction of the Service".). *FISS*: Government Regulation 330 on the FISS, article 6.2 ("to request and receive information necessary for taking decisions on the issues referred to the Service's competence"). *ROSCOM*: Government Decision NO. 110, article 7(d) ("to request on a free-of-charge basis from the federal executive bodies and from territorial bodies thereof, from executive bodies of Federal Subjects and local self-government bodies, as well as from the persons exercising activities in the area of communication, necessary data and materials concerning the exercise of control and supervisory authority of the Federal Service for Supervision in the Area of Communication").

exemption in law is clear, and the evaluation team does not consider this exemption an impediment to the FISS's ability to carry out its supervisory responsibilities. In practice the assessment team detected no obstacle to the FISS's ability to obtain information necessary to carry out its supervisory duties, and other enforceable means do provide the FISS with the authority to compel all information, regardless of financial secrecy provisions.

392. The AML/CFT Law is somewhat imprecise in its definition of competent authority and may leave Russia open to legal challenges by FIs claiming violations of bank secrecy provisions. The AML/CFT Law stipulates that the submission of information on all operations subject to both obligatory and suspicious reporting by all FIs to the "authorised body" will not constitute a breach of relevant secrecy laws. Government Ordinance No. 186[97] states specifically that the "authorised body" is Rosfinmonitoring and various regulations and directives issued by the BoR and the FSFM support this narrow interpretation. Depending on the legal interpretation, supervisory authorities (other than Rosfinmonitoring) that receive information under the AML/CFT Law directly from reporting entities may be in violation of financial secrecy provisions. Nonetheless, the AML/CFT Law allows for federal authorities, including the BoR, to provide information upon request to Rosfinmonitoring without breaching any secrecy laws.

393. Information sharing between private entities (including financial institutions) is prohibited except in certain permitted circumstances, which are set out in law[98]. Article 6 of this law states, that a private citizen's consent is not needed to share personal data when one of the following relevant conditions is met:

- A Federal Law specifies the justification for obtaining the personal data, the group of subjects whose personal data will be processed, and powers of the operators obtaining the data.
- The execution of an agreement, where the personal data of a party is required.
- Personal data may be shared when postal communications operators require personal data to deliver items of mail, electronic communications operators require data to settle payments with users for services provided.

394. As the requirements for information sharing between financial institutions and Russia Post are set out in a Federal Law (the AML/CFT Law), private entities are permitted legally to exchange personal information in this context per one of the conditions listed in the law.

395. The FIU and all state agencies involved in combating ML/FT are obliged to provide information to competent international authorities only on the basis of a bilateral or multilateral agreement (see section 6 of this report).

Effectiveness

396. The FIU and supervisors, with the exception of the FISS, have the appropriate and necessary legal powers to override confidentiality provisions in all situations where ML/FT concerns exist. Despite the exemption in the law for the FISS, all supervisors appear to use these powers on a regular and appropriate basis. Financial institutions, including insurance companies, seem well aware of the scenarios in which AML/CFT concerns override confidentiality provisions and indicate a broad willingness to comply with the reporting requirements.

3.4.2 Recommendations and Comments

397. The assessment team recommends that Russian authorities address the uncertainty regarding the definition of "authorised body" in the AML/CFT Law to ensure that all supervisors are covered.

---

97 Government Ordinance no. 186 "Issues of Rosfinmonitoring", paragraph 1.

98 Federal Law "On personal data" no. 152-FZ (of 27.07.2006).

3.4.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**C**	• This Recommendation is fully observed.

3.5 Record keeping and wire transfer rules (R.10 & SR.VII)

3.5.1 Description and Analysis

Recommendation 10 (Record keeping)

398. Article 7 of the AML/CFT Law only requires financial institutions to retain documents and data related to transactions subject to mandatory or suspicious reporting requirements for a period of at least five years following the termination of the business relationship. The following information must accompany transaction records subject to retention requirements:

- Type and purpose of transaction.
- Date and amount of transaction.
- Information related to the identity of the natural or legal person requesting the transaction.
- Information related to the identity of the beneficiary requesting the transaction.
- Information related to the identity of the representative conducting the transaction on behalf of the customer.
- Information related to the addressee/recipient of the transaction.

399. The Accounting Law[99] requires all organisations located in Russia, as well as their overseas branches and representative offices, to retain all primary account documents (including transaction records), accounting ledgers, and bookkeeping information for at least five years after their creation (article 7). However, these provisions do not require the keeping of documents for at least five years after the termination of a business relationship. The Accounting Law also does not specify what components of the transactions are necessary to be recorded.

400. While the AML/CFT Law and Accounting Law set requirements for record keeping of transaction records, the Federal Law on Archive Activity No. 125-FZ sets the national requirements for organisations to retain certain documents for specified periods of time. Article 6, paragraph 3 of this law authorises the Federal Archive Service to establish a list of specific documents and the corresponding retention requirement. This list, which carries the force of a regulation, includes specific mention of business correspondence and requires organisations to retain such correspondence for five years, although it is not specified whether this is from creation or from termination of the business relationship. The requirement to maintain account files is considered to be covered by the account documents requirement of the Accounting Law, but only for 5 years after their creation. The AML/CFT Law (article 7, item 4) requires FIs to retain all CDD information for at least 5 years following the termination of the relationship.

Reconstruction of transactions

401. Letter No. 99-T issued by the BoR informs credit institutions that transaction records subject to retention requirements, as well as other related documents and business correspondence, may be used as evidence in a criminal, civil, or arbitration proceedings, while Recommendation No. 983R issued by the government informs non-credit financial institutions of this stipulation.

[99] Federal Law no. 129-FZ "On Accounting".

Rosfinmonitoring Order 104 on Internal Control Procedures instructs all non-credit institutions to record all information related to transactions such that all the details related to the operation (including the amount of the transaction, currency, and data on participants in the transaction) may be used as evidence in criminal, civil, and arbitration proceedings. According to Resolution N 613/P of the FSFM, participants in the securities market must be prepared to reproduce all data available on a recorded operation at any time in the event that the information is needed to support a criminal investigation.

Timely access

402. The AML/CFT Law, article 7, paragraph 7, provides the Government and the BoR (for credit institutions) the authority to establish the procedure for financial institutions to provide information to the supervisory bodies. Each of the supervisory authorities have issued orders, implementing regulations, and other instructions to further articulate the requirement for financial institutions to provide information to supervisors either within the timeframe specified by an inspecting team or within a set period of time (*e.g.* no later than 15 days as required by the FSFM). However, as the specific requirement for timely access is not laid out explicitly in law or regulation, the assessment team determines that this criterion is not fully met.

403. With regard to reporting requirements, the AML/CFT Law does establish that financial institutions must report all transactions subject to mandatory or suspicious transaction reporting requirements no later than one working day following the date of the operation, and this kind of information must also be made available to the authorised authority upon request. The AML/CFT Law only specifies this requirement with respect to transactions subject to mandatory or suspicious reporting. However, the Accounting Law allows law enforcement authorities, the prosecutor's office, courts of law, tax inspectorates, and the internal affairs bodies to seize primary account documents from all organisations active in Russia (article 9, item. 8). See for general law enforcement access to documents Section 2.6, for supervisory access see Section 3.4 of this report.

Effectiveness

404. Based on on-site interviews of representatives from a broad spectrum of financial institutions, FIs appear to be well aware of and in compliance with the requirement to retain records subject to mandatory or suspicious transaction reporting requirements for a minimum of five years following the termination of the business relationship. Some credit institutions have established internal control procedures to retain all transaction records for at least five years from the date of termination of the business relationship, but this practice exceeds the current requirement established by law. While there is no specific mention in the relevant body of law and regulation requiring "timely access" to customer and transaction information, the evaluation team determined that the FIU and the supervisory authorities are generally satisfied with the timely nature of reports and reported no widespread compliance problems in obtaining information from reporting entities upon request.

Other enforceable means (effectiveness)

405. Aside from the legal framework set out in the AML/CFT Law and Accounting Law, Russia has taken some additional measures in other enforceable means that enhance the effectiveness of the system. CIs are required to retain business correspondence and messages for five years after the termination of the business relationship, and all other FIs have to keep correspondence documents and miscellaneous documents for at least five years following the termination of the relationship (BoR Letter 99-T and Order 104, item 2.8. Securities market participants are required to maintain internal registration records of all transactions for five years (FSFM Order No. 32 / MoF Order 108n, section 1, item 4 and item 13). CIs are required to produce documents requested by the supervisory authorities on a timely basis based on BoR Instruction 105-I (item 2.6) for CIs and FSFM Order 07-107/pz-n (item 15.2) for Securities Markets (time frame set by supervisor).

Special Recommendation VII (Wire transfers)

406. The current legal framework for implementing Special Recommendation VII in Russia is based on an amendment to the AML/CFT Law that has been in force since 15 January 2008. While the amended law appears to address gaps in the pre-existing legal framework governing wire transfers, the new provisions are cursory and do not address the resulting inconsistencies with the regulations (Regulations 2-P and 222-P on non-cash settlements)[100].

407. The amended AML/CFT Law covers all designated entities, but is only relevant to credit institutions, payment acceptance and money transfer providers (as referred to in article 13.1 of the Banking Law) and Russia Post. The following framework applies for all entities. The BoR provides specific guidance to credit institutions and ROSCOM provides specific guidance to Russia Post regarding their provision of both domestic and cross-border wire transfer services. (See below for additional information on Russia Post.)

Originator Information

408. The AML/CFT Law[101] requires that all wire transfers (*cashless settlements*) and *money transfers* (cashless settlements not originating from an account) carried out within Russia, or originating from Russia, be accompanied in all cases by originator information and an account number (when originating from an account). The law specifies that originator information must include name, family name, patronymic (or otherwise) and taxpayer identification number for natural persons. If the originator does not have a taxpayer number, then the originator must include an address or date and place of birth. For legal entities, originator information must include a name and taxpayer number or a foreign organisation code (AML/CFT Law, article 7, item 1.3). All entities designated by the AML/CFT Law must refuse any money transfer (to include both cashless settlements and money transfers not originating from an account) not accompanied by required originator information.

409. The originator information as required by the Russian law does not fully match the requirements of Special Recommendation VII. The FATF requirement for name and account number is covered, but there is no direct legal requirement to substitute the account number with another unique reference number if no account number is available. In some cases, a taxpayer identification number could serve as a unique reference number when an account number is not available. However, there is no provision to require another type of unique reference number if an originator lacks both a taxpayer number and an account number.

---

100 The evaluation team took into account changes in the legal framework that were in force within 2 months after the second on-site. The updated AML/CFT Law itself is an example of this. However, Regulation 2-P and 222-P were issued on 22 January 2008, but only in force 10 days later, thus these two regulation are outside the scope of this evaluation. The authorities made the team aware of the change in the AML/CFT Law, and the team received a copy of the proposed amendments and discussed the changes with the authorities during the on-site visit. The team was, however, not aware of the amendments to the Regulations until 4 months after the on-site, when the authorities provided the assessors with a copy of the amended Regulations.

101 AML/CFT Law, article 7, item 1.3 was translated as follows:
"Cashless settlements and money transfers without opening an account carried out on the territory of Russia and from Russia abroad, except those mentioned in item 1.1 of the present Article, shall be accompanied at all stages of carrying them out with originator information and the number of an account where the account exists through indication of that information in the settlement document or otherwise. The information on the originator – physical person shall include a name, family name, patronymic (if otherwise does not follow from law or national custom), as well as taxpayer identification number (if any) or the address (registration address) or place of living, or date and place of birth. The information on the originator – legal entity shall include the name, taxpayer identification code or foreign organisation code. The organisation carrying out operations with monetary funds or other assets shall refuse to conduct the money transfer in case of absence of information mentioned in paragraphs one-three of the present item."

410. In addition to the AML/CFT Law, BoR Regulations No. 2-P and 222-p govern domestic rouble-denominated transfers between credit institutions. The identifier information requirements set out in the AML/CFT Law (as amended) are consistent with the existing BoR regulations in that the new law requires domestic transfers to include originator information (name and taxpayer identification number or address) as well as some form of account information at every stage of the transfer. The BoR regulations require the ordering bank to collect the following information for the payment forms ("settlement documents"):

- The name of the settlement document and the code of the form.
- Number of the settlement document, day, month and year of issuance.
- The type of payment.
- Payer's full name, account and taxpayer identification number.
- Name / location of the payer's bank, bank identification code (BIC), correspondent (sub-) account.
- Recipient's name, account and taxpayer identification number.
- Name / location of the recipient's bank, bank identification code (BIC), correspondent (sub-) account.
- The purpose of the payment (for tax reasons).
- Amount of payment specified both with digits and in words.
- The priority of payment.
- Type of operation in accordance with accounting procedures of the BoR and CIs located in Russia.
- Signature(s) of authorised person(s) and stamp impression (in specified cases).

Domestic and Cross-Border Wire Transfers

411. Domestic and cross-border transactions are treated in the same manner under the AML/CFT Law. The AML/CFT Law defines cross-border transactions as transactions from Russia; incoming cross-border transactions are not covered by the Law and could not benefit from a requirement to adopt effective risk based procedures for transactions that lack full originator information, if such a requirement existed in Russia.

412. All specific types of transactions excluded from CDD and STR reporting requirements (below a threshold of RUB 30 000, see Section 3.2 of this report) are also exempted from these specific provisions. The threshold permitted for Special Recommendation VII is EUR / USD 1 000. As of the last day of the on-site visit to Russia (23 November 2007), RUB 30 000 represented a value of EUR 831, which is below the threshold, and USD 1 233, which is above the threshold. Considering that Russia's main trading partners are in the Euro zone, the evaluation team considers the threshold in line with the Standard.

Other elements

413. The authorities did not identify any technical limitations that preclude credit institutions from ensuring all originator information accompanies cross-border wire transfers. Therefore, all originator information can be transmitted with each transfer. Even if technical limitations were to prevent all originator information from being included with wire transfers, Russia's record keeping requirements under the AML/CFT Law and the Accounting Law should ensure that the receiving Russian institution will keep a record of the transaction.

414. The AML/CFT Law is silent on the issue of batch transactions. The Russian authorities confirm that batch transfers do exist in the Russian system but take the position that batch transfers must be accompanied by the full set of originator information since the law does not provide for simplified requirements for batch transfers (as permitted by this Special Recommendation).

415. Beneficiary FIs are not directly required to adopt risk-based procedures for identifying and handling wire transfers not accompanied by complete originator information, however the AML/CFT Law requires FIs to refuse a wire transfer if it is not accompanied by complete originator information. Given the gap between originator information as required by Russian law and as mandated by the FATF standard, and also given that the AML/CFT Law does not apply to cross-border wire transfers coming into Russia, the requirement to simply refuse transactions with incomplete originator information is not sufficient to protect against higher risk wire transfers. The BoR issued a letter in May 2007 to inform CIs of the Wolfsberg Group's proposals to reduce the risk associated with cross-border wire transfers, but has issued no additional guidance to credit institutions regarding risk-based procedures. Despite this lack of specific risk-based guidance, the assessment team notes that Russia's AML/CFT Law requires financial institutions to treat wire transfers as any other transaction and therefore they are subject to all existing mandatory and suspicious transaction reporting requirements.

Russia Post

416. There is no maximum limit set in law or regulation on the amount of money that can be transferred via the post, but the average transaction is usually valued at under USD 100. Russia Post sets the tariff schedule for all postal money transfers. According to representatives from Russia Post, their customer base is mostly comprised of elderly Russians, migrant workers, illegal immigrants, and those seeking to remit money to bordering countries. The size and cost of transactions going via the post is typically much smaller than wire transfers conducted via credit institutions.

417. Russia Post conducts cross-border wire transfers only with those countries with which it has a memorandum of understanding, which includes countries within the Commonwealth of Independent States (Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Ukraine and Uzbekistan), the Baltic countries (Latvia, Lithuania, and Estonia), France and China. The Post also has agreements with Turkmenistan, Georgia, Uzbekistan, Tajikistan and Lithuania to conduct "hybrid transfers," which involve an electronic transfer order that is received by the beneficiary post office via a postal transfer.

Supervision and Sanctions

418. The BoR is responsible for monitoring the compliance of CIs with all provisions of the AML/CFT Law, including those that apply to wire transfers. As Russia treats wire transfers the same as all other transactions subject to the AML/CFT Law, relevant sanctions would apply to both natural and legal persons. ROSCOM is responsible for supervising Russia Post. The assessment team received no information regarding sanctions levied against credit institutions or Russia Post specifically related to wire transfer violations.

419. Since the amendments to the AML/CFT Law regarding wire transfers entered into force after the on-site visit, the evaluation team was not able to discuss or assess the supervisory practice of the BoR or ROSCOM regarding these new provisions in the law.

420. The framework described in Section 3.10 of this report in relation to Recommendation 17 (sanctions) and 23 (monitoring and supervision), equally applies to this section.

Effectiveness

421. As the amendments related to wire transfers took effect on 15 January 2008, which was after the on-site visit to Russia, the evaluation team has no basis to evaluate the effectiveness of the new law. Further, Russia's supervisory bodies that oversee credit institutions and Russia Post do not appear to maintain separate statistics on sanctions levied for violations of wire transfer laws, so it is difficult to assess the effectiveness of Russia's supervisory and sanctions regime to date.

3.5.2 Recommendations and Comments

422. Record keeping requirements are generally comprehensive, but there are a few gaps in law and regulation, *i.e.* account files and business correspondence must only be kept for five years from their creation and not five years from the termination of the business relationship, and timely access is not defined. The assessment team recommends that Russia address these gaps in the legal regime. Also, the current legal regime requires financial institutions to ensure compliance with several different – and seemingly unrelated – laws and regulations. To ease the burden on reporting entities, the assessment team advises Russia to update the AML/CFT Law to include all necessary record keeping requirements, even if this duplicates requirements set out in other laws. The assessment team found that financial institutions are generally complying with record keeping requirements, and supervisors are taking effective measures to assess compliance in the course of their AML/CFT duties. The evaluation team did not receive any indication that any of the competent authorities had a problem obtaining the required information on a timely basis. Thus, the assessment team has raised the rating for this recommendation on the basis of effectiveness.

423. Overall, the new system governing wire transfers is a welcome step towards compliance, but significant gaps remain. The assessment team recommends that the Russian authorities amend the current AML/CFT regime to address the following deficiencies:

424. The definition of originator information may well be sufficient in the context of the Russian payment system framework, but it does not fully cover all requirements set by the FATF.

425. Incoming cross-border wire transfers are not covered by a requirement to adopt effective risk based procedures for incomplete originator information, and this vulnerability is not mitigated by the argument (as provided by the authorities) that most incoming cross-border wire transfers originate in countries that are largely compliant with FATF recommendations.

426. The BoR should provide specific guidance to credit institutions regarding the application of wire transfer regulations to batch transfers. Russia should develop rules requiring financial institutions to apply a risk-based procedure for wire transfers that lack full originator information. As a matter of effective implementation, if Russia amends the current law to include incoming cross-border wire transfers, Russian authorities will need to reconsider the current blanket requirement to simply refuse all transactions without full originator information as this could theoretically result in a complete halt to all incoming cross-border wire transactions.

427. The shortcomings described under Recommendations 17 (sanctions) and 23 (monitoring and supervision) for the banking sector / BoR and Russia Post / ROSCOM also apply to this section.

3.5.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**LC**	• Account files and business correspondence do not have to be kept for a minimum of five years from the termination of the account or the business relationship. • "Timely access" is not required by law or regulation.
SR.VII	**PC**	• Full originator information is not required in certain limited cases. • No requirements for beneficiary FIs to adopt a risk-based procedure for wire transfers, and incoming transfers are not covered at all. • Requirement to refuse transactions without full originator information cannot be implemented. • Batch transfers are not specifically mentioned in the Law. • Shortcomings identified under Recommendation 17 (sanctions) and 23 (monitoring and supervision) apply equally to this Special Recommendation. • Effectiveness of the new system cannot be measured.

3.6 Monitoring of transactions and relationships (R.11 & 21)

3.6.1 Description and Analysis

Recommendation 11 (Attention to unusual transactions)

Description and analysis

Special attention to complex and unusual transactions

428. FIs are required to establish identification criteria for extraordinary (unusual) transactions. In addition, in the case of a transaction with an intricate or unusual character that does not appear to make any economic sense or that does not has an evident legal purpose, the necessary information must be documented (AML/CFT Law, article 7, item 2).

429. In addition, certain transactions must be reported to the FIU if the amount equals or exceeds RUB 600 000. Many of the criteria that trigger an obligatory control report describe *de facto* unusual transactions (*e.g.* withdrawal from or placement in an account of a legal entity of cash funds when events are not consistent with the character of its economic activity). However, there is no general criterion that might permit subjective judgement; the list drawn up by the government is considered to be exhaustive. This remains a gap in the Russian system (AML/CFT Law, article 6).

430. Rosfinmonitoring Order 104 (only applicable to non-CI FIs) calls on financial institutions to develop identification criteria for unusual transactions, based on the recommended list of unusual transactions included in Appendices 2 and 3 of the Order. Although the Order only makes "recommendations", the evaluation team believes it qualifies as a sufficient requirement to pay special attention to complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose (further: unusual transactions). The criteria contained in the Appendices have to be taken into account by financial institutions. Corresponding breaches can be qualified as violations of the current legislation for which administrative liability is established in the form of fines (article 15.27 Code on Administrative Offences). Nonetheless, as with the AML/CFT Law, the Order lists certain criteria that should be taken into account, but it does not oblige FIs to look for other unusual transactions that may occur. This is a gap in the system.

431. Other, similar requirements and a list of recommended unusual transactions are included in Order 983R (applicable to non-CI FIs), Letter 99-T (applicable to CIs) and Order 613-R (applicable to securities market).

Examination and record keeping of complex and unusual transactions

432. Financial institutions are not required to examine as far as possible the background and purpose of detected unusual transactions. The AML/CFT Law requires financial institutions only to record the information obtained when applying the internal control rules but does not extend to the examination of unusual transactions (AML/CFT Law, article 7, item 2).

433. If an unusual transaction has been discovered in the activities of a client a CI may a) ask the client to provide the necessary explanation to clarify the economic sense of the unusual transaction; b) study all of the operations of this client made through the CI; c) perform other necessary action, provided that the legislation of Russia is observed (Letter 99-T, item 2.4.5, only applicable to CIs). However, there is no explicit requirement to examine as far as possible the background of unusual transactions and to set forth the findings in writing. First, CIs are not required to do so ("the CI may"); second, the CIs can choose one option out of three and third, the CIs are not required to set forth the findings in writing.

434. Since examining transactions is not required, FIs are also not explicitly required to make the corresponding findings available to competent authorities. Nevertheless, the AML/CFT Law establishes that the documents containing data on the implementation of internal control programmes should be kept for at least five years from the day when the relationship with the customer is cancelled (AML/CFT Law, article 7, item 4).

Effectiveness

435. All financial institutions seem to pay special attention to unusual transactions in practice. Some of them, mainly credit institutions, use special software to detect such transactions. Even though there is no legal requirement, in practice some FIs also examine as far as possible the background and purpose of detected unusual transactions and set forth the results in writing. In these cases, the relevant information is also available for competent authorities. However, not all FIs have such a practice. In addition, the evaluators had the impression that some FIs, when detecting unusual transactions, focus mainly on the requirements to report certain transactions equal to or exceeding RUB 600 000 based on mandatory monitoring – and not so much on subjective elements like unusual behaviour compared with the background of a specific customer. The fact that the law and regulations only list possible types of unusual transactions without pointing at the possibility of other kinds of unusual transactions does not raise the effectiveness of the system either.

Recommendation 21 (Countries that apply the FATF Recommendations insufficiently)

Description and analysis

Special attention to countries

436. FIs are required to file reports on transactions subject to mandatory control if the amount equals or exceeds RUB 600'000 and if at least one person involved is domiciled in a state that "does not participate in international AML/CFT co-operation". The list of such states (territories) is determined by the FIU, but in fact corresponds to the NCCT list of the FATF. Thus, at the time of the evaluation, there were no more countries that required special attention (AML/CFT Law, article 6 item 1, sub item 2 & Resolution 173[102]). Irrespective of the empty list, there is no explicit requirement to pay special attention to all transactions and business relationships with persons from or in countries that do not or insufficiently apply the FATF recommendations.

[102] Government Resolution no. 173 of 26.03.2003.

437. For CIs only, Regulation 262-P establishes that operations with residents of states or territories, about which it is known from international sources that they do not comply with the generally accepted AML/CFT standards, are deemed as high risk transactions. CIs have to devote special attention to transactions of this nature (Regulation 262-P items 2.9, 2.9.2, 2.9.12 and 2.9.13). This requirement would basically meet one element of the Recommendation. However, the evaluation team understood that the BoR has not issued a separate list of such countries. In isolated cases specific warnings against particular CIs from a third country were issued. However, these warnings were not specifically related to countries that do not or insufficiently comply with the FATF recommendations (BoR Letter 171-T, issued on 11 December 2003, and 15-T, issued on 31 January 2003, that refer to revoked licences (not for AML/CFT reasons) with respect to a list of banks in two countries).

Examinations of transactions

438. FIs are not required to examine as far as possible the background and purpose of business relationships and transactions with no apparent economic or visible lawful purpose from countries that do not or insufficiently apply the FATF Recommendations. The law requires FIs only to record the information obtained when applying the internal control rules, but does not extend to the examination of the aforementioned business relationships and transactions. Since there are no written findings, FIs are also not required to keep these available for competent authorities. Nonetheless, internal control data have to be kept available for at least five years (AML/CFT Law, article 7, item 2).

Countermeasures

439. According to the Russian authorities they are able to apply appropriate countermeasures and as an example, the evaluators were given BoR Letter 171-T (December, 2003). However, this letter only informed Russian banks of the fact that one of the countries listed by the FATF as an NCCT country had revoked the banking licences of a number of legal entities because of a lack of physical presence in the country. Even though the distribution of the list of legal entities is to be commended, this does not constitute a countermeasure against a country that does not or insufficiently applies the FATF Recommendations. The evaluation team did not receive any other past examples from the authorities of countermeasures against countries that would be satisfactory. Nevertheless, Russia indicated that the Law on Special Economic Measures enables Russia to apply countermeasures in accordance with Recommendation 21, if the FATF were to decide to apply countermeasures.

Effectiveness

440. The list of countries that "do not participate in international AML/CFT co-operation" issued by the FIU is currently empty because it is linked to the FATF NCCT-list. However, Recommendation 21 requires more than just a link to the list of NCCTs. In this regard, Recommendation 21 is, *de facto*, currently not applied by Russia. The evaluators did not find cases where the FIs had created their own lists of countries that do not or insufficiently apply the FATF recommendations either.

3.6.2 Recommendations and Comments

Recommendation 11

441. Russia should require FIs to examine as far as possible the background and purpose of all unusual transactions and to set forth the findings of such examinations in writing and to keep such findings available for competent authorities and auditors for at least five years. Russia should additionally make sure that FIs are no longer confused about the distinction between mandatory threshold reporting (> RUB 600 000) and examining the background of unusual transactions. Also, Russia should provide more guidance to the FIs, especially to make clear that the types of unusual transactions listed in laws and regulations is neither exhaustive nor closed.

Recommendation 21

442. Russia should require FIs to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. FIs should also examine as far as possible the background and purpose of business relationships and transactions with persons from or in those countries, to set forth the findings of such examinations in writing and to keep these findings available for competent authorities and auditors for at least five years.

443. Since Russia has indicated that it has the necessary legal framework through the new Law on Special Economic Measures, it should use this framework to apply countermeasures, as envisaged by Recommendation 21.

444. As a matter of urgency, Russia should establish a set of countermeasures that it can require the FIs to take in case a country continues to disregard the FATF Recommendations.

3.6.3 Compliance with Recommendations 11 & 21

	Rating	Summary of factors underlying rating
R.11	**PC**	• No requirement for FIs to examine as far as possible the background and purpose of all unusual transactions. • No requirement for FIs to set forth the findings of such examinations in writing. • No specific requirement for FIs to keep such findings available for competent authorities and auditors for at least five years. • Lack of effectiveness, especially in the non CI sector.
R.21	**PC**	• No requirement for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. • No requirement to examine as far as possible the background and purpose of such business relationships and transactions, to set forth the findings of such examinations in writing and to keep such findings available for competent authorities and auditors for at least five years.

3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)

3.7.1 Description and Analysis

Recommendation 13 and Special Recommendation IV (Suspicious transaction reporting)

Description and analysis

Requirement to make STRs (ML and FT)

445. The AML/CFT Law requires the reporting of suspicious transactions in ML cases. If an employee of an FI has any suspicion that the transaction could have anything to do with the laundering of criminal proceeds, the FI is required to report this transaction to the FIU no later than the next working day. The law explicitly refers to "proceeds of crime", which includes all crimes as stated in the CC. However, not all the 20 categories of designated FATF predicate offences fall into the category of serious crimes: insider trading and market manipulation are not covered by the CC (see Section 2.1) (AML/CFT Law, article 7, item 3).

446. The same article includes a requirement to file STRs in the case of a suspicion of financing of terrorism. However, shortcomings in the criminalisation for terrorist financing (see section 2.2 of this report) limit the reporting obligation**.**

447. FIs have to report not only suspicious transactions, but also certain transactions that equal or exceed RUB 600 000 ("mandatory reporting" or "reports on obligatory control"). Many of the criteria that trigger an obligatory control report describe *de facto* unusual transactions (for example withdrawal from or placement in an account of a legal entity of cash funds when events are not consistent with the character of its economic activity) that could also qualify as suspicious transactions. During the interviews with the private sector, it was not always clear if FIs understood the difference between unusual transactions (as discussed under Recommendation 11), mandatory threshold reporting or suspicious reporting. Most certainly, however, this was due to translation problems and not due to a misunderstanding of the law.

448. All suspicious transactions must be reported to the FIU pursuant to item 3 of article 7 of the AML/CFT Law.

Attempted transactions and tax matters

449. The reporting requirements to the FIU do not specifically refer to attempted transactions. The legislation seems to cover attempted transactions within an existing business relationship, but not attempted transactions of occasional customers. It should be pointed out that the second Mutual Evaluation Report of Russia by MONEYVAL identified this shortcoming. As a result, transactions that are refused by the FI have to be reported. That still leaves the possibility of occasional transactions aborted before the CI has refused to perform the transaction (AML/CFT Law, article 7.13).

450. There is no indication in the Russian legislation that STRs should not be filed if tax matters are involved. If there is a suspicion of ML or of TF, an STR must be filed, even though the reported transactions might not lead to a conviction for ML, since not all tax offences are predicate offences for ML (AML/CFT Law, article 7, item 3).

Additional elements

451. STRs are required to be filed if there is a suspicion that funds are the proceeds of any criminal act that would constitute a predicate offence in Russia. Insider trading and market manipulation do not constitute a predicate offence in Russia.

Effectiveness

452. The authorities provided the following statistics.

Reports by Credit institutions (1 149 institutions)					
Year	**2003**	**2004**	**2005**	**2006**	**Up to 1 Oct. 2007**
Mandatory reports	647 222	1 071 640	1 456 518	2 270 844	1 982 368
STRs	303 218	655 267	1 542 141	3 773 734	3 864 841

453. These figures show a constant growth of reports in recent years. In addition, many of the reports based on mandatory control also qualify as suspicious transactions. However, in interviews with the credit institutions it appeared that in some cases, reports were filed not because of a real suspicion, but only because the mandatory threshold was met. In other cases, an STR and a mandatory control report were filed for the same transaction. Nonetheless, all in all, the evaluators found that the system is established and works well with respect to credit organisations.

454. The following figures were provided for non-CI FIs.

Reports by non-CI FIs (January 2005 – October 2007) (number of institutions between brackets)				
Year		**2005**	**2006**	**2007**
Securities markets (1 678)	**Mandatory reports**	2 103	4 329	4 689
	STRs	328	847	2 376
Investment and pension funds (1 345)	**Mandatory reports**	788	787	914
	STRs	92	72	142
Post Russia (1) **(941 branches and 40 678 offices)**	**Mandatory reports**	1	1 218	2 025
	STRs	67	271	985
Insurance sector (863)	**Mandatory reports**	1 943	5 292	4 711
	STRs	33	346	1 193
Leasing companies (2 690)	**Mandatory reports**	40 496	70 631	83 439
	STRs	311	334	1 155

455. The number of reports from the rest of the FIs is much lower than for CIs, except for leasing companies. The trend is positive and the number of reports is generally increasing. The lower level of reports from non CIs compared to CIs reflects also the lower risk these entities run. For example in the insurance sector, there are in almost all cases small periodic premium payments accepted with a corresponding lower risk. In addition, the evaluators were told that these sectors are just developing, so very little money is channelled through these FIs. Furthermore, CIs have to file more reports based on *mandatory control*, so that the figures for CIs and non CIs are not absolutely comparable. Nevertheless, during the interviews with some of these other FIs, the evaluators sometimes had the impression that, not only are these sectors just developing, but also the awareness and knowledge about the AML/CFT regime is relatively limited. There was sometimes little familiarity with possible ML and TF threats and typologies relevant to their respective sector. Thus, the evaluators are of the view that some work should still be done in the non CI sector.

456. The number of STRs filed on the basis of a suspicion for terrorist financing is 2 104 in 2004, 9 603 in 2005 and 24 947 in 2007. The increased reporting of TF transactions demonstrates the increasing awareness of this issue, especially in the Southern Federal District (close to Chechnya) and the Central Federal District. Almost all the TF STRs were filed by credit institutions. More detailed statistics are provided below.

Number of reports related to TF 2004 – 2006 Breakdown per region				
Federal District	**Type of report**	**2004**	**2005**	**2006**
FEFD	Mandatory reports	0	3	0
	STRs	62	321	658
	Regional total	62	324	658
VFD	Mandatory reports	8	24	5
	STRs	268	1 054	2 460
	Regional total	276	1 078	2 465
NWFD	Mandatory reports	158	270	65
	STRs	117	1 003	3 052
	Regional total	275	1 273	3 117

Number of reports related to TF 2004 – 2006 Breakdown per region				
Federal District	**Type of report**	**2004**	**2005**	**2006**
SiFD	Mandatory reports	24	27	28
	STRs	158	636	1 577
	Regional total	182	663	1 605
UFD	Mandatory reports	22	37	37
	STRs	99	490	1 759
	Regional total	121	527	1 796
CFD	Mandatory reports	140	254	344
	STRs	405	2 351	6 487
	Regional total	545	2 605	6 831
SFD	Mandatory reports	37	107	383
	STRs	606	3 026	8 092
	Regional total	643	3 133	8 475
All Russia	**All reports**	**2 104**	**9 603**	**24 947**

Number of reports related to TF 2004 – 2006 Breakdown per reporting entity (FIs only)				
Financial institution	**Type of report**	**2004**	**2005**	**2006**
Credit institutions	Mandatory reports	389	722	860
	STRs	1 709	8 861	24 034
Securities	Mandatory reports	0	0	0
	STRs	3	8	21
Investment and pension funds	Mandatory reports	0	0	0
	STRs	0	3	3
Russia Post	Mandatory reports	0	0	1
	STRs	1	3	5
Insurance	Mandatory reports	0	0	1
	STRs	2	6	22
Leasing companies	Mandatory reports	0	0	0
	STRs	0	0	0
Total	**All reports**	**2 104**	**9 603**	**24 947**

457. Given the absence of any TF guidance, the evaluation team asked the authorities what would be typical situations where they would expect FIs to file TF STRs. The answer remained unclear. The interviewed financial institutions were asked the same question and often reference was made to the

terrorist lists under UNSCR 1267, which is not a sufficient response. The authorities explained that in practice, often a transfer of a small amount of money from a region with supposed TF activities or a withdrawal of a small amount of money from an ATM in such a region triggers an STR. Thus, in most of the cases of TF STRs there is no "real" TF suspicion. Based on this information, the evaluation team must therefore conclude that there is a lack of effectiveness in the TF STR system.

Recommendation 14 (Safe harbour and tipping off)

458. Reporting suspicious transactions by personnel of the reporting FI is not considered to be a breach of official, banking, tax, commercial or communication secrecy, provided that the transaction is reported for the purpose and based on the procedures of the AML/CFT Law (AML/CFT Law article 7, item 8). Because notionally there is no breach of secrecy, the personnel of the reporting FI are protected from both civil and criminal liability for breach of any restriction on disclosure of information, even if an STR was not filed in good faith. The only precondition is that an STR should be made for the purpose and based on the procedures of the AML/CFT Law. This precondition should be met in all the cases of STRs.

459. It should be noted that the reporting obligation is imposed on the FI, while the safe harbour provision exclusively protects the employees that report a transaction. This means that the FIs and their directors do not enjoy this safe harbour provision. Directors are not included in the term "employees". The translation of the relevant Russian provision relates clearly to "employees". Furthermore, Article 11 Labour Code stipulates that this Code does not apply to members of the board of directors of organisations, except for persons who have concluded a labour contract with the given organisation. In the opinion of the evaluators, therefore, a director who has not concluded a labour contract is not covered by the safe harbour provision. This could be less of a problem for FIs that are legal entities in criminal cases keeping in mind that there is no criminal liability for legal persons in Russia anyway. The lack of safe harbour would be a problem for FIs in administrative and civil cases and for directors in criminal, administrative and civil cases however.

460. Tipping off is prohibited by the AML/CFT Law which states that employees of the FI that report to the FIU do not have the right to inform the customers of the FI or other persons about the reporting. This provision is insufficient, as it only covers the employees, but not the FI itself nor its directors. This means that there is no provision that prohibits the FI and its directors from tipping off (AML/CFT Law, article 7, item 6). The Russian authorities stated that article 4 of the AML/CFT Law includes a clause to prohibit FIs from tipping off. The evaluation team has not accepted this because there no direct prohibition for FIs, their directors and employees. This Article only stipulates that measures against ML and TF shall include "banning on informing clients and other persons on measures taken against ML and TF".

Additional elements

461. Employees of the FIU are required to ensure the confidentiality of data protected by banking, tax or commercial secrecy, and are responsible for disclosing such information in accordance with the legislation (article 8 AML/CFT Law).

Effectiveness

462. The FI or one of its directors who files an STR is neither included in the safe harbour provision, nor covered by the tipping off provision. However, the negative influence on effectiveness seems to be limited. With respect to the safe harbour provision, there is no criminal liability for legal entities anyway, but the limited safe harbour provision could be a problem for FIs in administrative and civil cases and in any case for their directors. To avoid these problems, FIs could be more reluctant to file STRs and this could impede the effectiveness of the reporting system.

Recommendation 19 (other types of reporting)

463. The Russian authorities have considered implementing a system whereby FIs would be required to report all transactions in currency above a fixed threshold. Ultimately, the authorities did not choose to introduce this reporting form. However, the considerations did result in the mandatory reporting regime for transactions of RUB 600 000 and higher.

Recommendation 25 (Feedback related to STR)

464. Feedback and guidance related to STRs is limited to *i)* designing reporting forms and instructions, *ii)* sending an acknowledgement of the receipt of a report and *iii)* publishing annual reports on activities of the FIU, that also contain statistical data and typologies. The legislation does not require Rosfinmonitoring to provide feedback to reporting entities, and reporting entities do not ask for feedback. Thus an important tool for helping reporting entities to refine and improve the quality of STRs is not being used.

3.7.2 Recommendations and comments

Recommendation 13 and Special Recommendation IV

465. Russia should criminalise insider trading and market manipulation, so as to enable FIs to report STRs based on the suspicion that a transaction might involve funds generated by the required range of criminal offences. Russia should also finally introduce a reporting obligation for attempted transactions by occasional customers. It is particularly worrying that Russia still has not solved this gap in its law, despite the fact that it was identified in previous mutual evaluation reports.

466. Russia should issue TF guidance to enhance the effectiveness of the system for filing TF STRs.

467. The awareness of the AML/CFT regime in Russia outside the CI sector is in some cases low and Russia should raise the awareness in the non-CI FIs at a minimum through an enhanced training programme. The training should not only focus on the legal obligations, but also include the reasons for establishing an AML/CFT system, as well as examples, typologies and cases.

Recommendation 14

468. Russia should extend the safe harbour provision and the tipping off prohibition to FIs and their directors.

Recommendation 25

469. Russia should extend the case by case feedback beyond the acknowledgement of the receipt of the STR. It should also urgently consider other examples of case-by-case feedback, as those examples listed in the FATF Best Practice Paper for feedback by FIUs. This should also enhance the effectiveness of the reporting regime, as described above.

3.7.3 Compliance with Recommendations 13, 14, 19 and 25 (criteria 25.2), and Special Recommendation IV

	Rating	Summary of factors underlying rating
R.13	**LC**	• No STR requirement in cases possibly involving insider trading and market manipulation. • No general STR requirement for attempted transactions by occasional customers. • Shortcoming in the criminalisation for terrorist financing limits the reporting

	Rating	Summary of factors underlying rating
		obligation. • Lack of effectiveness, specifically relating to the TF STR system.
R.14	**PC**	• FIs themselves and their directors are not covered by the safe harbour provision and the tipping off prohibition.
R.19	**C**	• This Recommendation is fully observed.
R.25	**PC**	• No case-by-case feedback beyond the acknowledgement of the receipt of the STR.
SR.IV	**PC**	• No STR requirement for attempted transactions by occasional customers. • Shortcoming in the criminalisation for terrorist financing limits the reporting obligation. • Lack of effectiveness, specifically relating to the TF STR system.

3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)

3.8.1 Description and Analysis

Recommendation 15 (internal controls)

470. General requirements for financial institutions to establish and maintain internal control procedures, policies, and controls to prevent ML and FT are laid out in the AML/CFT Law. Specifically, article 7 of the AML/CFT Law requires financial institutions to develop internal control rules and appoint officials responsible for ensuring these rules are carried out. The law mandates that all internal control programmes include procedures governing the retention of documents, provisions for protecting confidential information, qualification requirements regarding staff and training of personnel on AML/CFT procedures. The law also requires internal control programs to include provisions that enable FIs to reveal and document "extraordinary operations," including operations with an "intricate or unusual character of an operation which does not have evident economic sense or evident legal purpose, the compliance of the operation with the goals of the organization, established by founding documents of this organizations" and specifies the requirements for an FI to report any suspicions detected during the implementation of established internal control procedures to the FIU. In practice, these provisions appear to relate to the need for internal control programs to incorporate requirements to retain documents related to STRs as well as to file STRs. All financial institutions must submit their internal control programmes to either BoR (CIs), FSFM (securities) or Rosfinmonitoring (all other) for approval. BoR Letter 99-T on Internal Controls instructs credit institutions to develop a training and educational programme for employees in AML/CFT internal control procedures. BoR Direction 1485-U further elaborates on this requirement and includes a comprehensive list of all those employees that must be trained on AML/CFT procedures and internal controls. (See below for further discussion of training programmes.) Annex 5 of Rosfinmonitoring Order 104 on Internal Control Rules applies to non-credit reporting organisations and recommends that the organisation familiarize its employees with the internal control rules that have been established by the organisation for AML/CFT purposes.

471. Various decisions, orders, regulations, and letters issued by the government, the FIU, BoR and other regulators further specify the required components of an internal control programme for FIs. Decision No. 983R instructs all non-CI FIs to ensure that internal control procedures contain provisions on CDD requirements, record retention, unusual and suspicious transaction criteria as well as reporting requirements, while Order 104 provides supporting detailed guidance on how to best implement these provisions. The AML/CFT Law authorised the BoR, in co-ordination with the FIU, to develop and adopt implementing regulations governing internal control programmes in CIs. BoR Regulation 242-P, Directive No. 1486-U, and Letter 99-T provide detailed recommendations for credit institutions on internal control programmes. For participants in the securities market, FSFM Order 613/r provides additional guidance on internal control programmes for the securities sector.

472. ROSCOM Order 459P, issued in September 2007, calls for each branch of Russia Post to establish internal control programmes. This order replaced a previous Order 507, which had been in place since 2005.

Designated AML/CFT Units

473. The AML/CFT Law requires FIs to appoint special officials responsible for implementing and ensuring compliance with internal control procedures, but delegates the authority for establishing the qualifying requirements for these officials to the Government and the BoR. Decision 983R calls for the "responsible official" to report mandatory or suspicious transactions to the "head of the organisation," who is responsible for making the final decision whether to submit the report to the FIU. Regarding CIs, the BoR issued Regulation 242-P, which instructs CIs to ensure that a "management body" oversees the internal control programme, and Letter 99-T, which calls for the "head of the credit organisation" to be solely responsible for a CI's AML/CFT compliance programme. In practice, the evaluation team found that most FIs had designated the CEO or the President as the "responsible official," while an identified staff member carried out the day-to-day compliance activities and reported directly to the senior executive.

474. ROSCOM Order 459P requires the head of the security department for each branch and regional office to serve as the "responsible official" charged with implementing the internal control programme. During on-site interviews with representatives from a regional office of Russia Post, the assessment team found that the representatives could not articulate clearly the structure of the compliance unit within the branch, nor could they describe clearly the system of internal control procedures in place at their branch. Also, the representatives stated that illegal migrant workers are among those who frequently use Russia Post to remit money to neighbouring countries, which would constitute a violation of Russia's CDD requirements and therefore indicates a significant deficiency in Russia Post's compliance function.

475. The Russian system provides the AML/CFT compliance officer and other authorised officials with appropriate access to information required in carrying out their duties. While there is no specific provision requiring timely access, there are various regulations and decisions which require financial institutions to allow compliance officials unimpeded access to all relevant information needed to implement internal controls. BoR Regulation 242 section 4.10 requires CIs to create conditions that would allow compliance officials with "uninterrupted and effective" conditions to ensure the full discharge of their duties to implement internal control procedures. In Letter No. 99-T, the BoR calls for CIs to allow the AML/CFT compliance officer to access any administrative or accounting documents; access any premises where data, cash, or computer processing equipment is stored; and order the temporary suspension of an operation in accordance with all Russian legislation. Order 104 calls for non-CI FIs to designate officials to receive information and documents from other employees in the organisation as well as all documents required to ensure implementation of the institutions' internal control programme. For the securities sector, the responsible official has the right to request any documents or information from any employee and to access any databases of the institution (FSFM Regulation No. 06-29/pz-n, item 5.1).

Independent Audit Programme

476. The AML/CFT Law requires financial institutions to establish the necessary organisational units to "effectively implement" the internal control programme. Various orders, directives and recommendations instruct FIs to vest the compliance officer with the responsibility to organise and implement programmes to ensure and verify compliance with internal control rules. The compliance officer is also responsible for providing a report at least annually to the head of the organisation on the results of the independent audit programme. While there is no explicit requirement in law, regulation, or other enforceable means that the independent audit programme must be adequately resourced, this requirement is implied by the repeated emphasis in the various laws, regulations and guidance regarding the need for the auditing function to be effective and comprehensive.

477. Article 42 of the Law on Banks and Banking Activities (No. 395-1) establishes that all CIs must have their statements and reports examined and verified by a licensed auditing organisation every year. The law specifies that these annual audits must evaluate a credit organisation's compliance with IC requirements and other mandatory norms established by the BoR, but this requirement appears to apply broadly to compliance with both prudential and AML/CFT matters. The auditing organisation must send its findings in writing to the BoR within three months of the presentation of the credit organisation's annual report to the BoR. Auditors have been informed that they must check an FI's compliance with all current legislation, including all relevant AML/CFT Laws[103].

478. Order 613/r (p. 5.6) requires all securities market participants to maintain a "programme of inspection (audit) of the internal control system with the aim of combating money laundering." The audit function should cover the organisation and implementation of both internal and external audit programmes, as well as a procedure for dealing with gaps identified by auditors. All other FIs are otherwise obligated under the Law on Auditing Activity No. 119-FZ to conduct an independent audit on their activity. Ministry of Finance Letter No. 07-05-06/302, dated December 19, 2006, specifically instructs all auditors to ensure that all audited entities also ensure compliance with AML/CFT legislation.

479. ROSCOM Order 459P, section 4.4 states that the Head of Security of each branch must submit quarterly written reports on the implementation of the postal branch's internal control procedures to the main Security Directorate of Russia Post. There is no information to indicate that Russia Post uses these quarterly reports from the branch offices to conduct an independent audit of country-wide implementation of internal control programmes.

Training Programmes

480. The AML/CFT Law as well as various regulations and other enforceable means establish clear requirements for all FIs to establish AML/CFT training programmes for relevant staff. Order No. 715[104], lays out the requirements for non-CI FIs to train and educate personnel in identifying customers and beneficiaries suspected of engaging in ML/FT. Both the BoR and the FSFM have issued guidance to CIs and participants in the securities markets recommending the establishment of regular training programmes for employees on AML/CFT. BoR Instruction 1485-U instructs CIs to establish a list of structural units within the organisation whose employees must undergo AML/CFT compliance training. The Instruction notes that this list should include, at a minimum, the following units: AML/CFT compliance unit, all units involved in banking operations and other financial transactions, legal units, the safety department and the internal control department. Based on interviews with various representatives from the financial sector, most institutions have established in-house training programmes and/or provide opportunities for employees to attend training conducted by the FIU or the relevant supervisory body. Of those banks visited during the on-site assessment, all had programmes in place to ensure that all employees, including tellers and all those involved in monetary operations as well as those directly responsible for AML/CFT compliance, receive training on AML/CFT.

481. ROSCOM Order 459P requires "persons responsible for internal control" to receive training at least once a year on AML/CFT and internal controls. On-site interviews with postal branches indicated that awareness of internal control programmes was low, indicating that few employees beyond the security staff receive any extensive training on AML/CFT compliance programmes.

482. While training seems to be offered across the board[105], the evaluation team perceived a particularly heavy focus on AML, with less of an emphasis on the warning signs associated with terrorism financing beyond checking the national list of terrorists and extremists. The team also noted

103 MoF Letter no. 070506/302, of 19.12.2006.

104 Government Order no. 715, 01.12.2005.

105 For example, Rosfinmonitoring trained 11 424 FI staff between 2003 - 2006 on the AML/CFT Law.

that almost all private sector representatives spoken to had a sufficient-to-good knowledge of the legal requirements, but very few could give an example of the kind of ML or TF cases seen in their sector nor could they explain the ML and TF threats relevant to their businesses.

Screening Procedures

483. The AML/CFT Law charges the BoR with determining the qualifications for employees responsible for ensuring compliance with the AML/CFT system. Order 104 instructs all non-CI FIs to establish qualification criteria for AML/CFT compliance officials that are in line with the requirements set forth by the government. Order 715 and BoR Directive 1486-U actually set forth these requirements for all FIs (e.g., responsible officials must have a higher education, the appropriate training on AML/CFT to complete their duties, no criminal record, etc.). Thus, the requirements for screening employees responsible for AML/CFT compliance are clear, but there are no broader screening requirements for all employees of an FI. As the Russian authorities admitted that most money laundering schemes in Russia could not take place without the complicity of financial institutions, the evaluation team viewed this lack of broader screening requirements as a deficiency in the overall AML/CFT regime.

Effectiveness

484. The legislative and regulatory framework adequately covers all FIs in requiring the development, implementation, and enforcement of internal control programmes. Based on statistics provided by the regulators as well as on-site interviews with representatives from the various types of financial institutions operating within Russia, CIs appear to have the most well-defined and adequately implemented internal control programmes in place. As CIs are arguably the most heavily regulated sector with respect to AML/CFT compliance, available statistics and anecdotal accounts from the regional supervisors show that the BoR has levied a correspondingly high number of violations stemming from insufficient or inadequate internal control programmes.

485. The evaluation team had a more difficult time determining the effectiveness of internal control programmes in non-CI FIs. Securities market participants and insurance companies appear to have well-structured programmes. The evaluation team met with a leasing company that appeared to have a comprehensive internal control programme in place. However, the company only carried out operational leasing which is not within the FATF definition of financial leasing, thus the evaluation team was not able to discuss issues relevant to effectiveness with this type of financial institution. Regarding ICs at Russia Post, both ROSCOM and representatives from Russia Post confirmed that the security department of each branch and regional office is responsible for developing, implementing and auditing the internal control programme, but the small number of violations seems inconsistent with the size of Russia Post. Also, on-site interviews with postal representatives revealed an inconsistent understanding of the internal control requirements set by ROSCOM, calling into question the effectiveness of the training programme as well as the internal control procedures themselves. As internal control programmes have, in theory, been in place at Russia Post since 2005, Russia Post should have been able to demonstrate fuller compliance with internal control procedures during the on-site interviews.

Recommendation 22 (Foreign Operations)

486. The AML/CFT Law does not include any provisions regarding foreign operations of Russian FIs. The Banking Law permits Russian CIs to open branches, subsidiaries, and representative offices provided that certain capital requirements are met and the BoR grants permission (Banking Law, article 35). According to the BoR, Russian CIs operate 13 subsidiaries in Europe and Central Asia; five branches located in China, India, Cyprus, and Greece; and 47 representative offices throughout the world.

487. The Banking Law also states that subsidiaries (not branches) must abide by the requirements of the BoR, so it could be inferred that foreign subsidiaries must apply the same AML/CFT provisions as the parent institution. Letter 99-T, issued by the BoR recommends that CIs with foreign branches establish requirements to observe know-your-customer principles in compliance with the laws of Russia at a minimum, but that branches should apply the laws of the country with the higher legal standard. However, this only relates to KYC, not to other AML/CFT requirements. The BoR has issued Instruction No. 76-I[106], but this instruction was not intended to deal with AML/CFT matters and applies solely to prudential considerations.

488. The BoR has not issued any guidance or instruction requiring CIs to apply a higher standard of vigilance for foreign operations in countries that do not or insufficiently apply the FATF Recommendations. Instead, the authorities have argued that the BoR will not license the creation of a subsidiary or a branch on the territory of a state that does not participate in the international AML/CFT regime, as determined by the law[107]. Currently, this provision is only linked to those countries on the FATF NCCT List. As this List does not name any jurisdiction at present, this provision does not sufficiently address the situation of those countries that indeed do not have adequate AML/CFT regimes in place. If a CI has already received a licence to operate in a country where the AML/CFT situation deteriorates below an acceptable level, the BoR states that this circumstance would be taken into consideration when the CI's licence comes up for renewal (every one to three years).

489. There is no specific provision instructing foreign branches or subsidiaries of Russian institutions to inform the BoR should the local laws or conditions inhibit compliance with Russia's AML/CFT Law. Russian authorities stated, however, that no foreign operation has encountered such a situation to date.

490. The evaluation team was not given any information about the rules for foreign branches and subsidiaries of non-CI FIs, even though the evaluation team learned from meetings with representatives from the insurance and securities sectors that they do have foreign branches and subsidiaries. Therefore, the evaluation team considers that this area is not covered.

Effectiveness

491. The current regulatory framework governing foreign operations of CIs is vague, at best, on AML/CFT matters, and requires financial institutions to infer their obligations with respect to foreign operations from regulations not specifically linked to AML/CFT matters. The lack of specific guidance requiring CIs to apply a higher standard of vigilance in countries that do not have adequate AML/CFT programmes in place puts those Russian CIs with foreign operations at risk to violations of Russia's AML/CFT regime. The evaluation team does not view the normal licensing renewal process as an adequate means of addressing those situations where a CI finds itself operating in a country where a significant deterioration in the AML/CFT regime has occurred. As such, the current legal and regulatory regime governing foreign operations of CIs is not effective or sufficient in meeting FATF standards.

492. As the current regulatory framework does not adequately cover foreign operations of non-CI financial institutions, the evaluation team cannot assess effectiveness of these sectors.

3.8.2 Recommendations and Comments

493. The Russian authorities should ensure that all FIs establish and maintain internal procedures, policies and controls to manage both AML/CFT and prudential risks, and to ensure that these policies and procedures are comprehensively communicated to all relevant employees. Financial institutions

[106] Instruction no. 76-I on the "Particulars of Regulation of the Activities of Banks which have set up Branches on the Territory of a Foreign State"

[107] BoR Regulation 290-P (of 04.07.2006) "On the procedure of granting by the BoR permission to credit intuitions to open subsidiaries on the territory of foreign countries".

and supervisory bodies should also ensure that training programmes incorporate case studies and other practical demonstrations of both money laundering and terrorism financing so employees are better able to detect signs of ML and FT when they occur. With respect to terrorism financing, FIs and supervisory bodies should amend internal control programme requirements to incorporate a more comprehensive approach to CFT beyond the current practice of simply checking the list of designated entities.

494. The Russian authorities should enhance existing provisions regarding employee screening procedures to ensure that all employees of FIs can be sufficiently screened. Considering that the Russian authorities believe that money laundering in Russia could often not take place without some complicity on the part of a financial institution, screening procedures should take criminal records into account, but should also assess the vulnerability to corruption of each employee or group of employees.

495. The assessment team urges ROSCOM and Russia Post to take proactive and comprehensive steps to ensure that all employees at all branches of Russia Post across the country have a good understanding of the Post's internal control programmes with respect to AML/CFT requirements of the ICP, and that compliance units are sufficiently trained and fully implementing all legal and regulatory requirements related to AML/CFT. The Russian authorities should work closely with Russia Post to ensure that the independent audit programme is being carried out effectively and comprehensively at all branches to verify compliance with internal control requirements across the country.

496. The Russian authorities should consider harmonising the existing legal and regulatory framework to ensure that all foreign operations – both branches and subsidiaries – of Russian FIs observe Russian AML/CFT requirements. Existing guidance for credit institutions on managing the risk associated with foreign operations should be expanded to address ML and TF risks as well as prudential risks. Russian regulators should consider issuing specific guidance to Russian credit institutions regarding the need for increased vigilance over foreign operations in jurisdictions that do not (or insufficiently) apply the FATF recommendations. As the Russian banking sector continues to grow and expand into the international financial sector, it will become increasingly important for Russian CIs to clearly and fully understand the AML/CFT requirements that apply to foreign operations. Further, FIs should be required to inform its Russian supervisor when a foreign operation is unable to observe appropriate AML/CFT measures because of local conditions.

3.8.3 Compliance with Recommendations 15 & 22

	Rating	Summary of factors underlying rating
R.15	**PC**	• Internal control procedures governing terrorism financing lack a comprehensive treatment of CFT, focusing almost exclusively on a "list-based" approach. • Training programmes of FIs focus too heavily on legal requirements under the AML/CFT Law, rather than on practical case studies of ML and TF, diminishing the effectiveness of the programmes. • Screening programmes are not broad enough, do not cover all personnel and do not focus on country specific risks, diminishing the effectiveness of the programmes. • Russia Post could not demonstrate effective implementation of internal control programmes at all branches.
R.22	**NC**	• The legal and regulatory framework does not consistently apply the requirement to abide by Russian AML/CFT Laws and regulations to both foreign branches and subsidiaries. • Existing guidance on foreign operations of CIs applies only to prudential risks, not to AML/CFT requirements. • There is no requirement for increased vigilance over foreign operations in jurisdictions that do not or insufficiently apply FATF recommendations.

	Rating	Summary of factors underlying rating
		• There is no specific requirement to inform the Russian regulator when a foreign branch, subsidiary or representative office is unable to observe appropriate AML/CFT measures. • Foreign operations of non-credit FIs are not covered by the existing regulatory regime, thus effectiveness of the current legal framework cannot be assessed.

3.9 Shell banks (R.18)

3.9.1 Description and Analysis

497. The Banking Law sets out certain requirements that must be met to establish a bank which effectively prohibit shell banks from operating within Russia. Article 1 establishes that a credit institution must be a legal entity with a physical address in Russia. All credit institutions must be registered with and have a licence issued by the BoR, and the BoR must affirm that the management of the bank is meeting Russian "fit and proper" standards. The BoR supervises the licensing process for all credit institutions and has the sole authority to grant and revoke banking licences. If the BoR determines that a bank provided false information during the licensing process, it can revoke a bank's operating licence.

498. Only CIs have the right to maintain correspondent relations with banks. According to item 5 of article 7 of the AML/CFT Law, Russian credit institutions are prohibited from establishing and maintaining correspondent relations with shell banks. Russian credit institutions are also required to take appropriate measures to ensure that they do not establish relations with foreign respondent financial institutions that allow their accounts to be used by shell banks.

Effectiveness

499. The evaluation team saw no indication that shell banks are operating on the territory of Russia. Further, interviews with representatives from credit institutions revealed that CIs are well aware of the prohibition against the establishment of correspondent relationships with shell banks.

3.9.2 Recommendations and Comments

500. This Recommendation is fully observed.

3.9.3 Compliance with Recommendation 18

	Rating	Summary of factors underlying rating
R.18	**C**	• This Recommendation is fully observed.

3.10 The supervisory and oversight system – competent authorities and SROs, Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)

3.10.1 Description and Analysis

Recommendation 23 (Regulation and supervision)

Regulatory framework (designated authorities)

501. AML/CFT regulations are set out in the AML/CFT Law which applies to all financial institutions (Art. 2 in connection with Art. 5 AML/CFT Law).

502. The following designated supervisory authorities have responsibility for ensuring that the financial institutions adequately comply with the requirements to combat ML and FT. See also section 1 of this report.

503. The BoR is the supervisor for CIs, which includes non-bank CIs [108].

504. The FSFM is the supervisor for the securities market ("professional securities markets participants"), investment funds and non-governmental pension funds[109].

505. The FISS is the supervisor for insurance organisations and insurance brokers[110].

506. ROSCOM is the supervisor for Russia Post (MVT)[111].

507. Rosfinmonitoring is the supervisor for leasing companies and payment acceptance and money transfer services (article 13.1 of the Banking Law)[112].

Criminal ownership

508. Russia has been criticised in past mutual evaluations[113] for being vulnerable to criminal ownership of financial institutions. While in the first report, it was found that organised crime might have penetrated the banking sector, the second report explicitly mentions the possibility that clandestine ownership of banks by organised crime was present, despite statutory provisions.

509. Disturbingly, Russia has not chosen to alter its laws to solve this issue. When a natural or legal person, through a single or multiple transactions, acquires more than 1% of the share equity of a credit institution, the BoR must be notified. If more than 20% is acquired, prior consent of the BoR is required (article 11 Banking Law and article 61 BoR Law). The BoR must communicate its decision within 30 days of notification, and a refusal must be "justified". The permitted justifications are as defined in article 11 of the Banking Law. It should be noted that criminal links or background may not be a reason for refusal, except in some cases (*e.g.* a conviction for intentional bankruptcy, inflicting loss on a credit institution). If the BoR does not reply to the request within 30 days, it is implicitly considered that consent has been given. Furthermore, these requirements do not extend to circumstances where a person owns less than 20% of the capital of the shares (stakes), but more than 20% of the voting rights, therefore, solely covering nominal ownership, but not control. In addition, the Banking Law does not contain further provisions about beneficial ownership. Taken together, all of these factors appear to indicate that the legal framework in Russia is not sufficient to help prevent criminals from gaining ownership or control of CIs.

510. While previous mutual evaluations have pointed to the possibility of criminal ownership of banks, the current evaluation team found that, through discussions with supervisory authorities, some banks are in fact still believed to be owned and controlled by (suspected) criminals and their front men. The authorities also indicated their strong and longstanding desire to obtain the necessary supervisory instruments to deal with this issue. However, legislative changes have not yet addressed this clearly identified weakness.

---

108 Federal Law on the BoR of 10.07.2002 no. 86-FZ and Federal Law on Banks and Banking Activities of 02.12.1990 no. 395-1 (Banking Law).

109 Federal Law no. 39-FZ of 22.04.1996 on the Securities Market, the Federal Law no. 156-FZ of 29.11.2001 on Investments Funds and Federal Law no. 75-FZ on Non-State Pensions Funds of 12.02.2001.

110 Federal Law no. 4015-1 of 27.11.1992 on the Organisation of Insurance Business in Russia.

111 Federal Law no. 176-FZ of 17.06.1999 and Federal Law no. 126-FZ of 7.7.2003 on Communications.

112 Government Regulation no. 28, 18.01.2003 / 03.11.2007) "On the procedure for registering entities in Rosfinmonitoring".

113 Second Mutual Evaluation Report of Russia (of 6 July 2004), Moneyval Committee of the Council of Europe.

511. With respect to the non-CI FIs, including those who offer money transfer services and leasing companies, there are no provisions regarding persons that hold a significant or controlling interest. This is also a longstanding concern of the international community. While the laws that apply to CIs at least create a legal framework, albeit without addressing criminal control adequately, the Law on the Securities Markets and the Insurance Law are completely silent on this issue and thus do not provide such a legal basis at all.

Fit and proper test

512. Persons who intend to hold a management function in a credit institution (including non-banking credit institutions) must be judged to be "fit and proper" by the BoR (article 11.1 and 16 Banking Law). This applies to the members of the board of directors (supervisory board), the head of a credit institution (the CEO, his deputies, and the members of the general management), the chief accountant, deputy chief accountants of a credit institution and also the head, deputy heads, chief accountant, deputy chief accountants of a branch of a credit institution. Candidates for the mentioned positions must meet qualification requirements established by federal laws and corresponding rules (other enforceable means) of the BoR with respect to fitness (expertise): higher education, working experience; with respect to properness (integrity): no convictions for economic crimes, business reputation, etc.

513. Similar fit and proper requirements apply with respect to professional securities market participants[114], joint stock investment funds[115] and non-state pension funds[116]. There are some requirements for the insurance sector[117], however, these fit and proper requirements do not extend to the members of the supervisory board. There are no fit and proper requirements with respect to leasing companies and commercial organisations according to article 13.1 Banking Law.

Effectiveness of criminal ownership and fit and proper test

514. The procedures with respect to fit and proper tests – where required – are effective. All relevant authorities are aware of the legal requirements and apply them in practice.

515. However, all the authorities need more legal powers with respect to preventing criminals from controlling financial institutions, especially against the background of the importance of this issue for Russia (see section 1).

516. As already recommended in previous mutual evaluation reports the FISS and the FSFM urgently need the power to check those who have a significant or controlling interests in a financial institution and their beneficial owners. The same is true for Rosfinmonitoring regarding leasing companies and commercial organisations according to article 13.1 Banking Law. This is for the moment probably less relevant for ROSCOM because the state owned Russia Post is today the only licensed institution in this area. Nevertheless, in theory it would be possible to issue such licences for other institutions. As the FISS, FSFM and Rosfinmonitoring do not have the competence to check major shareholders, they do not do so in practice.

517. The BoR is acutely aware of the need to preclude criminals from gaining control of credit institutions. This also extends to checking whether the owners' equity stems from appropriate sources. However, the legal powers of the BoR need to be strengthened. The threshold of 20% appears too high and should be lowered (even though this is not a direct requirement of the FATF Recommendations) taking into consideration the enhanced risk Russia faces in this area as already recommended in earlier

[114] Article 10.1 of the Law on the Securities Market and item 3 of Government Decision no. 432 of 14.07.2006 on Licensing Individual Types of Activity in Financial Markets.

[115] Article 8 of the Law on Investment Funds and item 3 of Government Decision no. 432.

[116] Article 7 of the Law on Non-State Pension Funds and item 3 of Government Decision no. 432.

[117] Article 2, 32.1 and 32.3 of the Law for re-insurance, mutual insurance, insurance brokers and insurance actuaries.

reports. In addition, it should be clarified that every person who, directly or indirectly, holds more than 10% of the shares or the votes of a credit institution should be checked as a major shareholder. Furthermore, it should be clarified that the BoR may refuse an acquisition if the concerned person was convicted for having committed a financial crime.

Core principles

518. All the financial institutions subject to the Core Principles are licensed (article 15 Banking Law, article 39 Law on Securities Market, article 2, 38 and 44 Law on Investment Funds, article 7 Law on Non-State Pension Funds and article 32 Insurance Law). The huge size of Russia poses a significant challenge to all the Russian supervisory authorities. Each supervisor is represented in each of the 7 Federal Districts (see section 1). For all supervisors, the Central Federal District (Moscow) has the largest number of FIs registered.

519. The procedure for scheduling on-site AML/CFT visits for the following year is basically identical for every sector. All the regional supervisory authorities in the Federal Districts propose a list of FIs to be inspected. Thereafter, a consolidated plan is drafted by the headquarters, based on the regional proposals. If necessary, the consolidated plan may be changed. In addition, the head of a regional office has the power to undertake unscheduled inspections. The regional offices report on a regular basis to the central office. In addition Rosfinmonitoring sends targeted information to the relevant supervisory authorities in relation to specific high-risk entities that it has identified through analysis of the FIU database.

520. In recent years, the following number of on-site visits have been carried out.

Number of on-site visits 2003 - 2006			
Institutions (total number as October 2007)	**Year**	**Number of on-site visits**	**Of which unscheduled**
Credit institutions (1 149)	2003	1 699	Unknown
	2004	2 592	Unknown
	2005	1 425	Unknown
	2006	1 419	Unknown
Securities management companies (including pension and investment funds) (2 164)	2003	171	Unknown
	2004	209	Unknown
	2005	198	Unknown
	2006	235	Unknown
Insurance (863)	2003	Unknown	Unknown
	2004	138	Unknown
	2005	164	Unknown
	2006	168	Unknown

521. The objective of the BoR is to conduct AML/CFT inspections for all CIs at least once every 18 months. The figures above demonstrate that this goal is met in practice. If necessary, the BoR also carries out unscheduled inspections. The evaluators got a sample inspection report, which showed into how much detail the inspections of the BoR go. It appeared that at least the sample report was very comprehensive. Overall, the evaluators concluded that the supervision carried out by the BoR works well and is effective.

522. The FSFM attempts to inspect all institutions under its authority at least once every two years. The figures above show that this goal is not reached in practice. On average, every securities market participant is only inspected once in nine to twelve years. Also with respect to the FISS, the goal that all insurance companies are inspected for AML/CFT matters at least once every three years could not be met. The figures above show that – on average – every insurance company is inspected only once in five to six years. It should be noted that Russia had submitted different figures for its MONEYVAL Progress report 2006[118] for the insurance sector (194 inspections in 2004 and 56 inspections in 2005) which calls into question the accuracy of these figures. The Russian authorities indicated that the difference in figures is due to the fact that the figures in the MONEYVAL follow-up report do not contain off-site inspections, as requested by the FATF evaluators. In addition, the figures for 2005 (56 inspections) refer to the 1st half of 2005 only.

523. In addition, the inspection reports the evaluators got from the FSFM and the FISS as a sample were much less comprehensive than the one from the BoR. To enhance the effectiveness, both authorities should carry out more on-site inspections related to AML/CFT to ensure that all institutions are inspected at least once every three years. In addition, both authorities should – on a risk basis – carry out more targeted in-depth thematic reviews.

Money or value transfer and money exchange services

524. Persons providing money or currency changing services must be licensed by the BoR. Thus, such services can only be offered by CIs. In practice, exchange offices that are structural units of credit institutions offer such money or currency changing services (Banking Law, article 5 clause 6). Foreign exchange services are monitored by the BoR, as any other CI. However, there are no separate statistics available with respect to the number of foreign exchange-related on-site inspections that concern exchange offices. The number of these exchange offices is constantly decreasing (2003: 4 237; 2004: 3 361; 2005: 2 835; 2006: 2 182; 2007: 1 475). The remaining 1 475 exchange offices are owned by 229 CIs.

525. CIs that provide MVT services are supervised by the BoR. As of December 2007, 1 135 banks and 43 non banking credit institutions had the right to provide MVT services in Russia. These 1 135 CIs include 3 474 subsidiaries, 18 275 additional offices (cannot be located outside the jurisdiction of the competent regional office of the BoR). 388 operational offices (may function on the entire federal district where the branch is located, but restricted in the types of transactions), 14 754 operational cashiers and 1 471 credit-cashiers offices (both even more restricted in the types of transactions they may conduct).

526. In addition, certain commercial organisations that provide specific types of services but are not CIs have the right to carry out money transfer services without a banking licence (article 13.1 Banking Law; see section 3.11). Russia implemented a registering requirement with Rosfinmonitoring for such organisations only on 3 November 2007 (after the first FATF on-site visit). On this date, Government Regulation No. 28 "On the procedure for registering entities in Rosfinmonitoring" was amended accordingly. During the first onsite visit, the BoR mentioned that these commercial organisations pose a big risk and that a system should be implemented to mitigate this risk. Order 183n that gave Rosfinmonitoring the power to supervise certain entities for AML/CFT purposes (including leasing companies) was replaced by Order 144 on 9 November 2007, adding these commercial organisations to the list of entities to be supervised by Rosfinmonitoring.

527. According to Rosfinmonitoring, as of January 2008, there were 58 such organisations registered, 9 supervisory visits took place in November and December 2007 and 271 operations, which were not reported to the FIU were detected, as well as infringements of internal control rules. The system to register and supervise commercial organisations according to article 13.1 of the Banking

[118] www.coe.int/moneyval.

Law is very young and thus it was not possible to evaluate its effectiveness. There is a need to consolidate this system.

528. Furthermore, Russia Post is allowed to offer money transfer services. Russia Post is registered with ROSCOM (article 29 of the Law on Communications; Government Resolution No. 318; Presidential Decree No. 320).

529. Russia Post is supervised by ROSCOM[119]. However, it remains unclear for the evaluators if the mentioned legal basis is sufficient (cf. R. 29). As of October 2007, 941 branches of Russia Post and 40 678 post offices existed. According to the authorities, every branch of Russia Post should be inspected on-site at least once every two years. The below mentioned figures show that this goal has not been reached and that every branch is only inspected once in five to six years regarding AML/CFT issues (at the same time the transactions of post offices can be checked as well). In addition, according to the documents that were presented to the evaluators to show the content and the depth of the inspections, the inspections are rather superficial and need to become more thorough to make them more effective. Some of the authorities in the regions mentioned a serious lack of staff.

Inspections of Russia Post by ROSCOMs				
Year	**Total number of inspections**	**Total number of AML/CFT inspections**		**Number of orders to correct deficiencies**
		Scheduled	**Unscheduled**	
2005	864	459	37	76
2006	1 663	46	141	10
2007	1 058	34	117	8
Total	**3 585**	**539**	**295**	**94**

530. Leasing companies are registered and supervised by Rosfinmonitoring. The following number of AML/CFT on-site visits have been carried out in the last years:

Inspections of leasing companies by Rosfinmonitoring *The total number of leasing companies is 2 690*		
Year	**On-site visits**	**Of which unscheduled**
2003	60	Unknown
2004	203	Unknown
2005	220	Unknown
2006	329	Unknown
Total	**812**	**Unknown**

531. These figures mean that a leasing company is visited only once in about eight to 13 years. This seems to be insufficient, also bearing in mind the rather large number of mandatory control reports and STRs from leasing companies and thus, the supposed potential higher risk in this sector compared to other non CI sectors.

[119] Item 5.3.1.2.5 of Government Regulation no. 354 of 06.06.2007 "On the approval of the Regulation on the Federal Service for mass media, communications and protection of cultural heritage".

Recommendation 25

Guidelines for financial institutions

532. Except for some limited guidance issued by Rosfinmonitoring (explanation of the law and typologies), no guidance has been issued. Not surprisingly, hardly any FIs had any knowledge of what constitute ML or TF, beyond the legal requirements of the AML/CFT Law.

Recommendation 29

Power for supervisors to monitor AML/CFT requirement

533. According to article 56 of the BoR Law, the BoR is the body in charge of banking regulation and banking supervision in Russia. According to article 73 of the BoR Law, in order to fulfil its regulating and supervising functions, the BoR inspects CIs (and their affiliates), addresses instructions to them to eliminate exposed violations in their activities and imposes sanctions against the violators in compliance with the BoR Law. At the first glance, it seems as if the BoR has adequate powers to monitor and ensure AML/CFT compliance and to conduct on-site inspections. However, as already identified in a previous mutual evaluation report (MONEYVAL), the BoR Law still limits the BoR in the number of on-site inspections it can carry out over a certain period. This limits the flexibility and the ability of the BoR to intervene, but it also provides temporary immunity from supervision to CIs, which is not in accordance with the FATF Recommendations (BoR Law, article 73/5)[120].

534. The FSFM and FISS have adequate powers to monitor and ensure AML/CFT compliance and to conduct on-site inspections[121]. The evaluation team was told that the powers of ROSCOM are based on article 27 of the Communication Law, on Government Regulation 354 and Government Decision 110. However, these provisions seem not to contain a sufficient basis with respect to controlling the full set of AML/CFT requirements. Government Decision 110 deals mainly with electronic communication issues. Item 5.3.1.2.5 of Government Regulation 354 is limited to the "observance by federal postal communication organisations of the procedure for recording, storing and provision of information on money transactions subject to control under the legislation of Russia, and also the organisation of internal control by these organisations".

535. The power of Rosfinmonitoring to monitor and ensure AML/CFT compliance with respect to leasing companies and commercial organisations according to article 13.1 Banking Law is based on Order No. 144 that replaced Order No. 183n on 9 November 2007.

Powers to compel production of records

536. The BoR has the power to compel directly – without a court order - production of and access to all records, documents or information relevant to monitoring compliance. The same is true for the FSFM[122].

---

120 The Law reads as follows: "In the discharge of the functions involved in banking regulation and banking supervision, the BoR has no right to carry out more than one check of the credit institution (of its affiliate) on one and the same questions over one and the same period of activity of the credit institution (of its affiliate), with the exception of the cases provided for by the present Article. The check may include only five years of activity of the credit institution (of its affiliate) preceding the year when the check is conducted".

121 Article 40 and 42, Securities Law, article 55 of the Law on Investment Funds, article 34 of the Law on Non-State Pensions Funds, Presidential Decree no. 314 and Government Decision no. 317, article 30 Insurance Law and Government Decision no. 330.

122 Article 73 BoR Law and Instructions of the BoR no. 105-I, article 44 of the Law On securities market, article 55 of the Law on Investment Funds and FSFM Order no. 07-108/pz-n "On approving the Regulation for conducting inspections of organisations, supervision and control for which the FSFM is the authorised body to exercise control and supervision" (items 3.4.3 - 3.4.6).

537. The FISS can request information as might be required to pursue insurance supervision, except for information deemed protected by banking secrecy provisions. The assessment team found, however, that this exemption is not related to the FISS's supervisory responsibilities and does not influence the powers of the FISS (see also description of Recommendation 4).

538. ROSCOM seems to have no such powers, as Government Decision 110 does not apply with respect to AML/CFT supervision.

539. Rosfinmonitoring has access to all relevant data of leasing companies and commercial organisations according to article 13.1 Banking Law pursuant to Order No. 144 that replaced Order No. 183n on 9 November 2007.

Powers of enforcement and sanction

540. For AML/CFT purposes, the supervisory authorities can independently impose the sanctions listed in the table below. In addition, all supervisors can request Rosfinmonitoring to levy a fine against the FI and the management, or disqualify (for up to three years) directors or senior management for non-compliance with a supervisory instruction [123].

Powers to sanction and fines				
Type of sanction	**BoR**	**FSFM**	**FISS**	**ROSCOM**
Sanctions against FIs for violation of AML/CFT-requirements	• Fine up to EUR 5 000 for CIs and up to EUR 500 for non bank CIs (article 74, p1 BoR Law) • Amount is multiplied by ten if the violation is not eliminated within the time period fixed by the BoR or if the violation has created a real threat to the interest of the customers (article 74, p 2 BoR Law)	• No power to impose fines	• No power to impose fines	• No power to impose fines
Sanctions against directors or senior management for violation of AML/CFT-requirements	• No power to impose fines on officials • Power to replace officials in cases of article 74, p 2 BoR Law	• No power to impose fines or replace officials	• No power to impose fines or replace officials	• No power to impose fines or replace officials
Restriction of the licence for violation of AML/CFT-requirements	• Up to 6 months in cases of article 74, p 1 BoR Law • Up to 1 year in cases of article 74	• No direct power for the supervisory authority for AML/CFT-purposes • Indirect power via	• No direct power for the supervisory authority for AML/CFT-purposes • Indirect power via	• No direct power for the supervisory authority for AML/CFT-purposes

[123] Article 19.5 and 15.27 Code of Administrative Offences.

Powers to sanction and fines				
Type of sanction	**BoR**	**FSFM**	**FISS**	**ROSCOM**
	item 2 BoR Law	Petition Court and Rosfinmonitoring for 90 day suspension (article 3.12 CAO)	Petition Court and Rosfinmonitoring for 90 day suspension (article 3.12 CAO)	• Indirect power via Petition Court and Rosfin-monitoring for 90 day suspension (article 3.12 CAO)
Withdrawal of the licence for violation of AML/CFT-requirements	• BoR may revoke a licence for repeated (one year minimum) violations of article 6 and 7 AML/CFT Law (except for not filing a STR) (article 20 p. 1 Banking Law) • Licence cannot be revoked for other reasons (article 20 p. 3 BoR Law)	• FSFM may revoke a licence for repeated (one year minimum) violations of article 6 and 7 AML/CFT Law (except for not filing a STR) (article 44 i. 4 Law on the Securities Market). • No corresponding provision in the Investment Funds Law, in the Law on Non-State Pensions Funds or Decision No. 317	• Not possible for AML/CFT-purposes	• Not possible for AML/CFT-purposes

541. The powers to sanction, as well as the sanctions themselves, are inadequate. The BoR, the only supervisor with some powers, indicated that their powers are too limited to effectively correct compliance shortcomings. The evaluation team fully agrees with the view of the BoR. The FISS and FSFM both denied having too limited powers, despite basically having no powers at all. It is unsure why FSFM and FISS choose to deny lack of powers.

542. The BoR is the only supervisor in Russia which is able to impose fines for violations of AML/CFT requirements and to replace (disqualify) directors or senior management. Additional indirect measures are available to supervisors to fine management and directors via Rosfinmonitoring (article 15.27 CAO). However, the evaluation team is of the opinion that the supervisory authorities should also have direct powers in such cases.

543. The maximum amounts available for fines against credit institutions for violations of AML/CFT requirements are too low.

544. A withdrawal of a licence for violations of AML/CFT-requirements is possible only in the banking and in the securities sector, and only for repeated violations during one year, with the notable being failure to file an STR with the FIU. In the evaluators' view, the exception regarding the filing of STRs and the precondition to have repeated violations in the course of one year unduly restricts the effectiveness of this measure and should therefore be abolished. In addition, it should be made clear that every supervisor has the competence to withdraw the licence of its financial institutions for violations of AML/CFT-requirements.

545. The MONEYVAL Second Mutual Evaluation Report recommended that Russia grant the BoR power to withdraw a licence when the owners or controllers are convicted for criminal or economic offences. This issue has not been resolved since then. The situation is the same for the FSFM, the FISS and ROSCOM.

Effectiveness

546. The BoR imposed the following sanctions in the last years:

Measures and sanctions applied by BoR (all figures)		
	Year	**Numbers**
Summary of deficiencies and breaches presented to the management of the institution)	2003	353
	2004	459
	2005	385
	2006	343
Instructions to eliminate identified breaches identified during an on-site visit within a fixed term	2003	135
	2004	142
	2005	373
	2006	389
Limit certain operations and restrict opening of new branches	2003	7
	2004	71
	2005	238
	2006	529
Penalties applied by BoR (only applied to legal persons	2003	81
	2004	105
	2005	284
	2006	232
Licences revoked	2003	0
	2004	2
	2005	14
	2006	51

Measures and sanctions applied by BoR (summary)		
Year	**On-site visits**	**Total of sanctions**
2003	1 699	576
2004	2 592	779
2005	1 425	1 294
2006	1 419	1 544

547. In addition, Rosfinmonitoring applied six sanctions in relation to credit institutions in 2004-2006, two of which were fines imposed on senior management (on the basis of files submitted by the Prosecution Authority).

548. The evaluators were told that, since 2002, the BoR had spent most of its time educating CIs but that currently, stricter sanctions are applied. This is reflected in the figures indicated above. Nevertheless, the figures for 2003 and 2004 are not satisfactory because these include preventive measures and instructions presented to eliminate violations. The figures for 2005 and 2006 prove that progress was made and that today, the system to sanction credit institutions works effectively, despite the defective legal framework.

549. The other supervisors for financial institutions imposed the following sanctions in the last years.

Measures and sanctions applied by other supervisors (all figures)				
		FSFM	FISS	ROSCOM
	Year	Securities, investment and pension funds	Insurance companies	Russia Post
Number of orders for breaches of the AML/CFT legislation sent to Rosfinmonitoring	2003	141	0	0
	2004	50	0	0
	2005	45	1	4
	2006	61	4	19
Number of orders on suspension of the licence for breaches of the AML/CFT legislation	2003	6	0	0
	2004	0	0	0
	2005	3	0	0
	2006	7	0	0
Number of orders on annulment of the licence for breaches of the AML/CFT legislation	2003	2	0	0
	2004	1	0	0
	2005	2	0	0
	2006	3	0	0
To compare: number of on-site visits	2003	171	0	0
	2004	209	0	0
	2005	198	164	496
	2006	235	168	187

550. Rosfinmonitoring has levied the following number of fines against FIs and their management (some based on files received from Supervisors and the Prosecution Authority). The number for leasing companies is substantially higher since Rosfinmonitoring is the sole supervisor for this sector.

Number of fines by Rosfinmonitoring						
Year	CIs	Securities	Insurance	Russia Post	Leasing companies	Article 13.1 Banking Law entities
2003	0	0	0	0	66	0
2004	3	1	0	0	229	0
2005	1	2	3	0	163	0
2006	2	7	13	1	295	0
Total	**6**	**10**	**16**	**1**	**753**	**0**

551. These figures show that the system for sanctioning non-CI FIs does not work effectively, especially with respect to the FISS and ROSCOM. The total number of sanctions does not appear to be commensurate with the number of on-site visits. The evaluators recommended that the FSFM, the FISS and ROSCOM should carry out more and more targeted in-depth thematic reviews. The figures regarding the number of sanctions seem to confirm that many of the on-site visits carried out by the FSFM, the FISS and ROSCOM are quite superficial.

552. While not a formal breach of the FATF Recommendations, it needs to be noted that ROSCOM will in practice never be able to revoke the single licence of the state-owned monopolist Russia Post. Nonetheless, when asked during the on-site visits, ROSCOM staff were always quite happy to point at the fact that revoking the licence was still the only measure they could take. All this limits the effectiveness of the supervisory powers of ROSCOM.

Recommendation 17 (Sanctions)

Designation of authority to impose sanctions

553. The BoR is able to impose fines on credit institutions for violation of AML/CFT requirements. The law sets the fines in EUR and not in RUB. The maximum fine is EUR 50 000 for banks and EUR 5 000 for non bank CIs. These amounts do not appear to be proportionate or dissuasive and should be raised substantially (article 74 item 1 and 2 BoR Law jo. Article 11 Banking Law).

554. In addition, for non-compliance with the AML/CFT Law requirements related to record keeping requirements and in relation to mandatory threshold reporting and internal control measures, the Code of Administrative Offences envisages the following sanctions for designated FIs (article 15.27).

- Administrative fine for officials of 100 to 200 times the minimum monthly wage of RUB 2 300 (maximum equals approximately EUR 12 000).
- For legal entities – a fine of 500 to 5 000 times the minimal monthly wage of RUB 2 300 (maximum equals approximately EUR 300 000).
- Administrative suspension of activities for up to 90 days.

555. Rosfinmonitoring is the competent authority for dealing with these cases, but such cases can also be transferred to a judge for consideration, who can also suspend the activities of an institution for up to 90 days (articles 3.12, 23.1 and 23.62, Code of Administrative Offences). Such suspensions have never been applied with respect to FIs**.**

556. It was not obvious to the evaluators that article 15.27 of the Code of Administrative Offences covers the main violations of the AML/CFT Law, particularly in the case of non compliance with CDD requirements. The Russian authorities explained that article 15.27 contains a punishment for breaches of internal control rules, which in the understanding of this term by Russian legislation (as stipulated by the numerous Regulations and Instructions of the Government, BoR, Rosfinmonitoring and FSFM) include a wide range of requirements, including customer identification. However, the evaluation team was not convinced by this explanation. In addition, while the maximum fine for legal persons seems to be adequate, this is not the case with respect to officials of FIs, even though it has been increased from 6 000 to 12 000 EUR.

557. There are no criminal sanctions available for violation of the AML/CFT Law.

558. Pursuant to article 74 of BoR Law, if a CI violates the legal requirements of the BoR, or if it does not or incompletely submits required information, the BoR has the right to demand that the CI

rectify the found violation, to impose a fine on the CI, or to impose restrictions on the performance of the individual operations.

559. In addition, the BoR has the right to order the replacement of the managers of the CI if the latter fails to meet deadlines imposed by the BoR instructions referring to violations, as well as if these violations or banking operations carried out by the CI have created a real threat to the interests of its creditors (depositors) (article 74 BoR Law).

560. The FSFM, the FISS and ROSCOM do not have powers to sanction their supervised entities.

Scope and proportionality of sanctions

561. The range of sanctions available in Russia with respect to CIs includes written warnings, orders to comply with specific instructions and suspension of the licence (article 74 BoR Law and article 15.27 Code of Administrative Offences). However, the framework needs to be fine tuned to ensure that it is applicable to AML/CFT breaches.

562. A withdrawal of a licence for violations of AML/CFT-requirements seems to be possible only in the banking and in the securities sector, except in cases where an FI did not file an STR with the FIU or repeated violations during one year. In the evaluators' view, the exception regarding the filing of STRs and the precondition to have repeated violations during one year is not adequate and should be abolished. In addition, it should be made clear that every supervisor has the competence to withdraw the licence of its financial institutions for violations of AML/CFT requirements.

Effectiveness

563. See Recommendation 29 above for an overview of sanctions and the ineffectiveness of the framework for the non-CI FIs.

3.10.2 Recommendations and Comments

Recommendation 23

Banking sector

564. Russia should – as a matter of urgency – strengthen the regime to prevent criminals from becoming major shareholders in a CI by amending the Banking Law to lower the threshold from 20% to 10%[124], by ensuring that every person who, directly or indirectly, holds more than 10% of the shares or the votes of a credit institution, is checked as a major shareholder and by ensuring that the BoR can refuse an acquisition if the concerned person was convicted for having committed a financial crime.

Other sectors

565. Russia should as a matter of urgency – and as already recommended in the Second Round Evaluation Report by MONEYVAL – implement provisions to prevent criminals from becoming major shareholders in a non-CI FI.

566. Russia should – also as a matter of urgency – raise the awareness of the staff of the FSFM, the FISS and ROSCOM and increase their number of staff substantially to ensure that every FI undergoes at least one on-site inspection every three years and that – on a risk basis – more targeted in-depth thematic reviews are carried out.

[124] The FATF Recommendations do not prescribe that the threshold should be 10%, however, the evaluation team deems that 10% is the appropriate threshold in the Russian context.

567. Russia should – still as a matter of urgency – consolidate and strengthen the system to register and supervise organisations providing MVT services according to article 13.1 Banking Law, including the implementation of fit and proper tests.

568. In addition, Russia should implement fit and proper tests for leasing companies and amend the Insurance Law to ensure that members of the board of a life insurance company or an insurance broker are fit and proper.

569. Furthermore, Russia should amend the Law on Communications to ensure that all conceivable money value transfer service providers are licensed or registered and supervised.

Recommendation 29

Banking sector

570. Russia should amend the BoR Law to elevate the maximum amount for fines against credit institutions substantively and to ensure that the BoR has the competence to impose adequate fines on directors and senior management of banks for violation of AML/CFT requirements.

571. In addition, Russia should amend the BoR Law to ensure that a licence of a CI can be revoked when the owners are convicted for a relevant criminal or economic offence and to ensure that a licence of a CI can also be revoked for not filing STRs with the FIU. Russia should also ensure that the licence of a CI can be revoked not only if repeated violations occur during one year and thus, amend the BoR Law accordingly.

572. Furthermore, Russia should abolish the limitation on the BoR to conduct on-site inspections in article 73 item 5 BoR Law, as already recommended in the MONEYVAL Second Round Report.

Other sectors

573. Russia should – as a matter of urgency - amend the relevant laws to ensure that the FSFM, the FISS and ROSCOM have the power to impose fines on their FIs and on directors and senior management of their FIs for violation of AML/CFT requirements and to replace directors and senior management of their FIs for violation of AML/CFT requirements.

574. Russia should – also as a matter of urgency - abolish the limitation of the FISS to compel and obtain access to banking secrecy information.

575. Russia should – still as a matter of urgency - increase the staff for the FSFM, the FISS and ROSCOM to ensure that the system for sanctioning financial institutions works effectively.

576. Russia should stipulate explicitly ROSCOM's competence to carry out on-site inspections with respect to the full set of AML/CFT requirements and to compel production of records.

577. Russia should in addition amend the relevant laws to ensure that a licence can be revoked for violation of AML/CFT requirements also in the non-banking and non-securities sectors, and when the owners are convicted for a relevant criminal or economic offence (concerns the FSFM, the FISS, ROSCOM and Rosfinmonitoring).

578. Russia should furthermore amend the Law on the Securities Market to ensure that a licence of a corresponding FI can also be revoked for not filing STRs with the FIU and abolish the precondition of repeated violations during one year to revoke a licence.

Recommendation 17

579. Russia should amend article 15.27 Code of Administrative Offences to ensure that the main violations of the AML/CFT Law are covered, especially regarding non compliance with the requirement to identify the customer and the beneficial owner and to elevate the maximum amount for fines against officials of financial institutions.

Recommendation 25

580. Russia should implement the requirement to issue guidance to FIs, beyond the explanation of the law.

3.10.3 Compliance with Recommendations 23, 29, 17 & 25

	Rating	Summary of factors relevant to s.3.10 underlying overall rating
R.17	**PC**	• Maximum fines that can be imposed by the BoR are too low. • Article 15.27 Code of Administrative Offences is not sufficiently broad. • Maximum fines against officials of financial institutions are too low. • No powers for supervisors (other than the BoR) to replace directors / senior management. • No powers for the BoR, the FSFM, the FISS and ROSCOM to withdraw a licence when the owners are convicted of a relevant criminal or economic offence. • System to sanction financial institutions other than credit institutions is not effective.
R.23	**PC**	• No provisions to prevent criminals from becoming major shareholders in a non-banking financial institution. • Inadequate threshold with respect to major shareholders of credit institutions. • Inadequate provision regarding persons having a controlling interest with respect to a credit institution. • No fit and proper requirement regarding leasing companies and the members of the board of a life insurance company or an insurance broker. • No fit and proper test and general lack of effectiveness regarding the system to register and supervise organisations providing MVT services according to article 13.1 Banking Law. • Lack of effectiveness with respect to the supervision of the FSFM, the FISS and ROSCOM.
R.25	**PC**	• Insufficient and ineffective guidance to FIs, beyond an explanation of the law.
R.29	**PC**	• Limitation on the BoR for conducting on-site AML/CFT inspections. • FISS not able to compel and obtain access to information protected by banking secrecy. • Maximum fines against credit institutions are too low. • No power for the BoR to fine directors or senior management. • No powers for the FSFM, the FISS and ROSCOM to impose fines on financial institutions and directors / senior management and to replace directors / senior management. • No powers for the BoR, the FSFM, the FISS, ROSCOM and Rosfinmonitoring to withdraw a licence when the owners are convicted of a relevant criminal or economic offence. • System to sanction financial institutions other than credit institutions is not effective. • Lack of clarity with respect to ROSCOM's competence to carry out on-site inspections related to the full set of AML/CFT requirements and to compel production of records.

3.11 Money or value transfer services (SR.VI)

3.11.1 Description and Analysis (summary)

581. The Banking Law (article 5 clause 9) licences CIs and select types of commercial organisations to provide MVT services in Russia. The Post and Communication Law licenses Russia Post to provide MVT services in Russia. These institutions are designated under the AML/CFT Law (article 5). As all legal entities within Russia, CIs, all commercial organisations, and Russia Post must be registered in the USRLE, which also includes information on licenses that have been issued to each legal entity.

582. All MVT service providers are included in the list of organisations required to comply with the AML/CFT Law. Compliance with Recommendations 4 (financial institution secrecy or confidentiality), 5 (CDD), 6 (PEPs), 7 (correspondent banking), 8 (non-face-to-face business), 9 (third party introducers), 10 (record keeping), 11 (monitoring of accounts and relationships), 13 (suspicious transaction reporting), 14 (tipping off), 15 (internal controls), 22 (foreign branches and subsidiaries), and 23 (supervision), and the corresponding deficiencies are described earlier in section 3 of this report.

583. All other forms of MVT service not specifically authorised by the Banking Law, including alternative remittance systems, are illegal and subject to criminal sanction.

Credit institutions

584. As of December 2007, 1 135 CIs are licensed by the BoR to conduct all forms of MVT services. CIs are licensed to perform money transfers on behalf of individuals without requiring the requesting individual to open a bank account. CIs are permitted to enter into agreements with payment acceptance service providers to effect money transfers, and operations conducted within the framework of these agreements are subject to the supervision of the BoR, which carries out supervision over all operations of credit institutions. In addition the BoR issued an instruction for CIs with respect to money transfers[125]. The BoR is responsible for ensuring that CIs apply all relevant AML/CFT provisions to MVT services, and is authorised to levy the appropriate sanctions when violations occur.

Non-bank credit institutions

585. The BoR licenses and supervises 43 non-bank CIs currently operating in Russia. These institutions fall into three main categories: (1) deposit-only institutions, (2) payment/settlement institutions (*i.e.* institutions that deal primarily with remittances, not including payment acceptance services) and (3) credit institutions. The BoR registers, licenses, and supervises non-bank credit institutions, as well as banks.

Payment acceptance and money transfer services providers

586. The Banking Law also allows a particular kind of commercial organisation known as "payment acceptance and money transfer services providers" (article 13.1) to provide cash transfer services under a set of specified circumstances. These providers may collect cash on behalf of individuals to effect payment to a third party for telecommunication services, residential accommodation and utility services. These entities do not require a licence to conduct these transfers and are not supervised by the BoR, but they must register with the FIU and are covered by the AML/CFT Law[126]. These institutions are allowed to conduct MVT services under two conditions: *i)* they must have a contract with a credit institution on whose behalf it is affecting the transfer, and *ii)*

[125] BoR Instruction 1842-U "On the mechanism of carrying out the transfer, of 20.06.2007).

[126] Article 5 includes "non-credit organisations accepting cash funds from physical persons in cases provided for by the legislation on banks and banking activity" as one of the organisations subject to the AML/CFT Law.

the credit institution must have a contract with the person rendering the service. By December 2007, 53 non-credit institutions providing these services had registered with Rosfinmonitoring.

Russia Post

587. Russia Post has a monopoly over all postal services in Russia. It is also licensed to provide remittance services. Russia Post is identified in the AML/CFT Law as an FI and must therefore comply with all the provisions of that law. ROSCOM is responsible for registering, licensing, and supervising Russia Post's compliance with AML/CFT requirements that apply to its provision of MVT services. ROSCOM issues one licence to Russia Post, and all postal operations fall within the scope of this licence. (See Section 3.5 for additional information regarding the volume and nature of postal money transfers.)

Effectiveness

588. Many of the same concerns expressed in Section 3.5 regarding the effectiveness of Russia's AML/CFT regime on wire transfers apply to money and value transfer services, as the same entities authorised to conduct wire transfers are also the only entities authorised to conduct money and value services - with the exception of specific types of non-credit commercial institutions (*i.e.* "payment acceptance service providers"). In November 2007, Rosfinmonitoring became responsible for registering, licensing and supervising these payment acceptance service providers. The Russian authorities demonstrated that Rosfinmonitoring has made a concerted effort since assuming this responsibility to register these entities and conduct supervisory visits, but the assessment team did not meet with any of these entities during the on-site and is therefore unable to assess the effectiveness of their AML/CFT compliance programs.

589. The current system provides fairly effective oversight of legal MVT service providers, but it does not effectively address the existence of illegal alternative remittance systems (ARS) operating in Russia. Given the size of the migrant worker population and the widespread use of ARS within Central Asia and the bordering countries, Russian law enforcement bodies and the FIU do not appear to be devoting sufficient resources to rooting out, investigating, and prosecuting ARS providers, nor is there any effort to work with migrant communities to establish legal alternatives to ARS. Russian law enforcement authorities provided information on some cases involving criminal prosecutions of "hawala"-type operations, but it is not clear whether Russian law enforcement authorities proactively seek to identify ARS operating within Russia that could possibly be used to finance terrorism or legalise criminal proceeds.

3.11.2 Recommendations and Comments

590. While Russia's banks are well-regulated and broadly apply all legal provisions to MVT, the BoR appears to provide only minimal oversight of non-banking credit institutions and statistics on enforcement actions against this category of MVT service providers are lacking.

591. As articulated in Section 3.5, the sprawling nature of Russia Post poses a challenge to effective enforcement of AML/CFT requirements that apply to money and value transfers. Russia should consider implementing laws and regulations to ensure that postal operations are better aware of and in compliance with the AML/CFT requirements. Suggested improvements would include: *i)* increased technical interface between postal branches to better detect suspicious transactions, *ii)* rules governing the volume and frequency of remittances permitted and *iii)* improved training of postal operators on AML/CFT. Given the size of the postal sector, Russia should also consider either increasing the capacity and quality of ROSCOM's compliance function or transferring supervisory and regulatory powers to another federal authority that is better equipped and trained to assess AML/CFT compliance.

592. As the state-owned Russia Post is the only postal service provider in Russia licensed to provide MVT services and ROSCOM grants only a single licence for all branches and offices in Russia, ROSCOM cannot effectively use its sanctioning power to address MVT violations found to have occurred at Russia Post. Russia should find creative ways to ensure that ROSCOM has sufficient powers to correct deficiencies found in Russia Post's AML/CFT compliance.

593. Russian law enforcement bodies should place a higher priority on investigating the existence of alternative remittance systems to better assess the size and the nature of ML/TF threat posed by illegal MVT occurring within and through Russia.

3.11.3 Compliance with Special Recommendation VI

	Rating	Summary of factors underlying rating
SR.VI	**NC**	• The current system lacks effectiveness in ensuring compliance. • Insufficient attention is devoted to the existence of and risks presented by illegal alternative remittance systems. • Payment acceptance service providers were not covered by supervisory regime until November 2007, therefore effectiveness of their compliance with AML/CFT rules cannot be determined. • Implementation of Recommendations 5, 6, 7, 8, 10, 13, 14, 15, 22 and 23 in the MVT sector suffers from the same deficiencies as those that apply to banks. • ROSCOM lacks effective sanctioning powers.

4. PREVENTIVE MEASURES – DESIGNATED NON-FINANCIAL BUSINESSES AND PROFESSIONS

594. Within the AML/CFT Law, Russia has set up two different regimes for Designated Non-Financial Businesses and Professions (DNFBPs). The first regime is set up for FIs, but it also includes the gaming industry, the real estate sector and dealers in precious metals and stones.[127] The rules under the AML/CFT Law for FIs, gaming, real estate agents and dealers in precious metals and stones are fully identical. Where possible, the description for the AML/CFT system for these two sectors is cross-referenced to section 3 of this report. Pawnshops are also part of the regime for FIs. However, since this activity is not a DNFBP activity under the FATF Recommendations, the sector is described in section 4.4 of this report.

595. The second regime that has been set up applies to lawyers, notaries and accountants. In general, the regime for these sectors is a less strict version of the system for FIs. The requirements for these three sectors are fully described in this section of the report. In all cases, the specific reporting requirements only apply to these professions if, during the course of business, the professional has any ground to assume that the aim of the operation or financial transactions is to launder money or finance terrorism (*i.e.* these professions have no obligations under the mandatory control requirements). In addition, the requirements only apply if the information or service that is provided is not covered by professional secrecy provisions in relation to the following activities:

- Real estate operations.
- Management of monetary funds, securities and other assets owned by the customer.
- Management of bank and securities accounts.
- Organisation of contributions for the creation of entities, ensuring their operation and management.

[127] See section 1 for breakdown of institutions and entities that are subject to the AML/CFT Law.

- Creation of entities, their operation and management as well as the purchase or sale of these entities.

596. It should be noted that this section of the report uses the terminology of the FATF Recommendations. This means that, even though the requirements of the Russian AML/CFT Law apply to the entire gaming industry, this report only refers to casinos.

597. The evaluation team was given no information about the activity of trust and company service providers (TCSPs[128]), which are not designated under the AML/CFT Law (but do exist, see section 1). As such, no separate analysis of this activity is included within the following sections. The evaluation team was initially given no information on accountants, except for the fact that this sector is designated under the AML/CFT Law and has apparently filed a small number of STRs. The authorities did not arrange a meeting of the evaluation team with representatives of the accountant sector, despite the requirements that have been set for the 3rd round of FATF Mutual Evaluations. The evaluation team considers therefore the requirements for TCSPs and accountants have not been implemented. Further information about the accountant sector was provided some time after the on-site visits.

598. Independent accounting activity in the understanding of the FATF Recommendations is carried out in Russia only by auditors and audit companies. In accordance with the Auditing Law, auditors may perform functions which are complementary to the audit, including accounting. Because auditors are the only type of activity licensed to perform accounting functions, in the context of this report they will be referred to as accountants. The MoF is the government authority exercising oversight over accountants (auditors). The MoF issues licences for their activity. Accountants are designated under the AML/CFT Law. In addition, the MoF has issued a letter, requiring bookkeepers (i.e. accountants) to use the broader AML/CFT legal framework available for other reporting entities, such as Government Regulation 983R[129].

4.1 Customer due diligence and record-keeping (R.12) (applying R.5, 6, 8 to 11 and 17)

4.1.1 Description and Analysis

Casinos, real estate agents and dealers in precious metals and stones

599. See sections 3.2 – 3.3, 3.5 – 3.6 and 3.10 of this report. All requirements for FIs set out in the AML/CFT Law and those contained in Order 104 and Decision 983R apply in relation to these sectors.

Effectiveness (casinos, real estate agents and dealers in precious metals and stones)

600. The evaluation team met with two dealers in precious metals and stones, neither of whom appeared to be technically covered by the FATF criteria (*i.e.* dealing in cash). Therefore effectiveness in this sector could not be assessed.

[128] See Section 1.3 for an explanation of the use of the term TCSP in this report.

[129] Auditing Law article 1, item 6, sub item 1, Government Regulation no. 80, of 06.02.2002, Regulation no. 329, of 30.06.2004 and Letter no. 07-03-01/647 of 27.06.2005.

601. The basic customer identification requirements under the AML/CFT Law appear to be applied in the real estate agent sector. However, it was of considerable concern to the evaluation team that the casino sector was not consistently applying CDD measures, with one casino indicating that full identification would not necessarily be taken and verified on the customer's first visit to the casino, although the customer would be allowed full access to gambling facilities. In addition, this casino thought that it had no right to ask for information relating to the source of the customer's funds, but it was happy to record its guests under fictitious names. Otherwise, the casinos spoken to carried out customer identification of all visitors upon entry, and customers are issued a membership card which is required when chips are purchased.

602. The change in the AML/CFT Law, which came into effect on 15 January 2008, introduces certain elements for assessing foreign public persons, but effectiveness could not be measured, given the newness of the provisions.

603. It is not clear whether the use of new payment technologies particularly affects these sectors, but there are no provisions except the need to personally identify all customers. Moreover, casinos are not allowed to make use of the internet or other communication technologies[130].

604. Casinos and real estate agents are aware of the need to keep records of identification data for at least five years, and most appear to be complying with this requirement.

605. Casinos and real estate agents appear to be treating the requirement to detect and record unusual transactions the same as those for recording transactions subject to mandatory control and reporting STRs. As for the financial sector, the effectiveness of compliance with Recommendation 11 is in doubt.

606. More generally, although sanctions have reportedly been imposed in all three sectors for breaches of customer identification provisions, the lack of specific detail about the nature of these breaches and the penalties imposed means that effectiveness cannot be judged.

607. Overall, the evaluation team has concerns about the effectiveness of the regime as it relates to the sale and purchase of real estate. There is the possibility of sales and purchases being registered directly with the land registry. The Russian authorities point out that the land registry is a government authority, which has a requirement to present to Rosfinmonitoring all the information contained in its database in accordance with Government Regulation 425. The authorities say that Rosfinmonitoring regularly requests information from this authority. It is, however, not clear to what extent this information is used to inform Rosfinmonitoring's work. Banks are required to report real estate transactions over certain thresholds in accordance with article 6 of the AML/CFT Law, however any sales under the threshold and any cash transactions would not be routinely reported.

Lawyers, notaries and accountants

608. The only requirement in relation to CDD is the application of identification requirements regarding the customer. For natural persons, the professional must establish surname, name, patronymic, citizenship, data on identification document, migration card, or residence permit, address (residence or temporary), and taxpayer's identification number. For legal persons a name, taxpayer's identification number or a code of a foreign organisation, state registration number, the place of state registration and the legal address are required (AML/CFT Law, article 7.1, item 1 jo. article 7, item 1, sub item 1). The Notary Code contains a requirement to carry out basic identification of all customers. This is separate to any requirement under the AML/CFT Law.

130 Law 244-FZ on Regulation of Gaming Activity, Item 3 of Article 5.

609. Separately for accountants, the MoF issued a letter[131] which requires these professions to abide by the provisions of Government Regulation 983R. This Letter also requires accountants to identify beneficiaries (item 2). Therefore the provisions of 983R apply to accountants in the same manner as to the financial institutions described in section 3. In addition, accountants are permitted to use an AML/CFT risk assessment in deciding whether or not to establish relations with a customer. The Code of Ethics of Auditors (accountants) states that before establishing a relationship an auditor must assess whether the client poses a risk to the professional integrity of the auditor. Dubious characteristics include participation of the client in illegal activity, defined as laundering of criminally gained proceeds (article 2.2). The auditor must evaluate the level of risk, and if this level is high, to undertake measures to eliminate or reduce the risks. These include obtaining more information about the client, its owners, internal control etc. The auditor may request from the client a guarantee letter pledging to improve corporate governance or strengthen internal controls. If the levels of risk cannot be brought to an acceptable level, the auditor must refuse the relationship. In addition auditors must "occasionally" review the risk-status posed by the client. (Code of Ethics of auditors (accountants), section 2, items 2.1-2.6). As the evaluation team was not able to meet with any auditors, it is impossible to judge how effective these measures are in practice.

610. The only requirement in relation to record keeping is to keep the data and documents that are necessary for the identification of the customer for at least 5 years after the termination of the relationship (AML/CFT Law, article 7.1, item 1 jo. article 7, item 1, sub item 4). Notaries are separately required to keep records of property transactions for a period of 75 years.

611. The AML/CFT Law contains a requirement that lawyers, notaries and accountants have internal control systems that enable them to reveal and document "extraordinary operations", including operations with an "intricate or unusual character of an operation which does not have evident economic sense or evident legal purpose, the compliance of the operation with the goals of the organisation, established by founding documents of this organisation", but there is nothing further dealing with complex, unusual large transactions or unusual patterns of transactions (articles 7, item 2 and 7.1, item 1).

612. The evaluation team was given no evidence that non-compliance with the CDD and record keeping rules has been sanctioned yet under the provisions of the AML/CFT Law. The Russian authorities consider that they have power to impose such sanctions under paragraph 2 of article 13. In addition, the legal and notarial professions both have codes of ethics under which transgressions of the identification requirement could, in theory, be sanctioned. Other than this, the evaluation team was not made aware of any other sanctions available. Accountants (auditors) fall under external oversight of the MoF in accordance with Article 14 of the Auditing Law, which gives the MoF power to verify "the quality of operation of individual auditors and audit organisations". The Russian authorities consider that any breach of existing Russian legislation by accountants may lead to a sanction, including the revocation of a licence, and that violation of the AML/CFT provisions contained in the Code of Ethics of auditors (accountants) can also lead to a sanction. The evaluation team was not made aware of any sanctions that had been imposed for breach of AML/CFT provisions, and was not able to meet with any accountants.

613. The AML/CFT Law specifies that lawyers, notaries and accountants should develop rules of internal control which, inter alia, should include "criteria of revealing and signs of extraordinary operations". In practice this appears to relate to the need to file STRs, although very few have been received. Additionally, MoF Letter No. 07-03-01/647 requires accountants to appoint AML/CFT compliance officials. The Lawyers' Chamber has reportedly issued Recommendations to its members on the implementation of the AML/CFT Law, but these were only provided to the evaluation team in Russian.

[131] Letter no. 07.03.01 no.647.

614. It appears that the new provisions relating to PEPs are not included in the requirements relating to lawyers, notaries and accountants.

615. There are no other requirements for lawyers, notaries and accountants in relation to Recommendations 5 – 6, 8 – 11 and 17.

Effectiveness (lawyers, notaries and accountants)

616. Lawyers, notaries and accountants are subject to a much reduced version of the general requirements in the AML/CFT Law. In particular, CDD requirements only extend to basic identification, and not to all of the requirements under Recommendation 5. Again, the lack of any provisions relating to PEPs until recently is an area of concern.

617. Arguably it is more likely that notaries and possibly accountants in Russia will be engaged in the activities covered by the FATF Recommendations, as lawyers have a more representational role. Notaries are involved in property transactions, but to a lesser extent since a change in the law now allows for property transactions to be recorded directly with the land registry without the participation of a notary.

618. The evaluation team was told that no actual sanctions have been applied in respect of lawyers. In respect of notaries, sanctions have been applied for breach of the identification requirement, but it was not possible to ascertain whether this had been strictly speaking the result of a breach in the requirements of the AML/CFT Law, or in the more general requirement in the Notary Code. Lawyers and notaries can be disbarred for breaches of their respective codes, but no such sanctions have been used for direct breaches of the AML/CFT Law. The indirect nature of the supervisory and sanctions regime raises questions about the effectiveness of the measures available. The authorities consider that the co-operation agreements between Rosfinmonitoring and the Lawyers' and Notaries Chambers are a positive move, but it is not clear to the evaluation team what practical effect these currently have.

619. The lack of guidance for all sectors on how the requirements of the AML/CFT Law affects them, how it interacts with their respective codes of ethics and what their members can expect by way of supervision and sanctions raises doubts about the effectiveness of the basic provisions in the AML/CFT Law.

620. As the evaluation team was not given the opportunity to meet with any accountants, effectiveness in this area could not be assessed.

4.1.2 Recommendations and Comments

621. Russia should review the AML/CFT regime as it applies to DNFBPs and ensure that all of the relevant criteria are addressed. For casinos, real estate agents and dealers in precious metals and stones, the basic recommendations set out earlier in this report in relation to Recommendations 5, 6 and 8-11 are applicable, as these entities are subject to the full effect of the AML/CFT Law in Russia. Where effectiveness is a concern (for example in relation to CDD in the casino sector), the consequences of failure to conduct CDD requires further attention.

622. The revised AML/CFT Law contains some of the criteria relating to Recommendation 6. Russia should ensure that the gaps in these requirements are covered by the legal framework specific to these sectors.

623. In relation to lawyers, accountants and notaries, specific provisions to address all of the relevant criteria in Recommendations 5, 6 and 8-11 are necessary. In particular, extending the CDD requirements to include their full range in the legislation. Russia should also take steps to examine ways of increasing the effectiveness of compliance with AML/CFT requirements in these sectors.

624. With a diverse range of supervisory bodies (Rosfinmonitoring, the Assay Chamber, the Federal Notaries Chamber and the Federal Lawyers Chamber) Russia should take steps to co-ordinate the overall approach in this area.

625. Russia should also examine the use of cash in the real estate sector in order to be sure that there are no important gaps in the AML/CFT system as it relates to this sector.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating

R.12	**PC**	*Applying R.5*
		• Casinos/Real Estate Agents/Dealers in Precious metals and stones – similar technical omissions as recorded under R 5. In particular:
		  ○ No requirement for dealing with doubts about veracity of previously obtained information.
		  ○ Lack of clarity and effectiveness in respect of beneficial ownership requirements.
		  ○ Lack of clarity in relation to ongoing due diligence.
		  ○ Doubts about clarity and effectiveness of requirements relating to SDD and EDD.
		  ○ Timing of verification – no requirements.
		  ○ Failure to complete CDD requirements limited to failure to carry out customer ID.
		  ○ Concerns about effectiveness in the casino sector.
		• Lawyers/notaries/accountants
		  ○ CDD requirements only relate to ID.
		Applying R.6
		• Lawyers/notaries/accountants: New provisions do not apply.
		• All other entities: similar omissions as recorded under R 6.
		Applying R.8
		• Casinos: requirements limited to prohibition of gambling via the internet.
		• All other entities: no requirements except the need to personally identify all natural persons.
		Applying R.9
		• N/A
		Applying R.10
		• Casinos/Real Estate Agents/Dealers in Precious metals and stones
		  ○ Similar omissions as recorded under R 10.
		• Lawyers/notaries/accountants
		  ○ No requirement to keep records except for those relating to ID.
		• Applying R.11
		• All designated assessed sectors
		  ○ Similar omissions as recorded under R 11, practice suggests concentration on factors which give rise to the submission of STRs.
		• All Recommendations: TCSPs are not covered.
		• Accountants – no information on effectiveness.

4.2 Suspicious transaction reporting (R.16) (applying R.13 to 15, 17 & 21)

4.2.1 Description and Analysis

Casinos, real estate agents and dealers in precious metals and stones

626. See sections 3.6 – 3.8 and 3.10. All requirements for FIs set out in the AML/CFT Law, Order 104 and decision 983R in relation to Recommendations 13 – 15 and 21 apply also in relation to these sectors. In particular, casinos and real estate agents are obliged to send written details of their internal systems and controls to Rosfinmonitoring for approval. A similar requirement relates to dealers in precious metals and stones, who send details to the Assay Chamber.

Lawyers, notaries and accountants

627. If a lawyer, notary or accountant, during the course of business, has any grounds to assume that the aim of the operation or financial transaction is to launder money or finance terrorism, then he is obliged to notify the FIU. Notification through a self-regulatory organisation (SRO) is optional, if that SRO has concluded an agreement with the FIU (for lawyers and notaries only). There are currently co-operation agreements between Rosfinmonitoring and both the Federal Chamber of Lawyers and the Federal Notary Chamber. However, both lawyers and notaries are obliged to submit STRs directly to Rosfinmonitoring. Both organisations informed the evaluation team that they were looking at the viability of STR reporting through them. Tipping off is prohibited (AML/CFT Law, article 7.1, sub items 2 – 5). The procedure for notifying the FIU is set out in Ordinance 82, and effectively mirrors the requirements of the AML/CFT Law.

628. Article 7.1.1 of the AML/CFT Law includes a requirement for lawyers and notaries to develop rules of internal control (by reference to article 7.2). These are general rules requiring staff training and the appointment of officials responsible for AML/CFT measures.

629. There are no other requirements for lawyers, notaries and accountants in relation to Recommendations 13 – 15, 17 and 21.

Statistics

Suspicious transaction reports		
	Year (for 2007: to Sept only)	**Number**
Gambling (total / casino only)	2005	22 / 21
	2006	178 / 162
	2007	52 / 31
Dealers in precious metals and stones	2005	2 503
	2006	1 185
	2007	212
Lawyers and notaries	2005	1
	2006	0
	2007	8
Real Estate agents	2005	0
	2006	82
	2007	220
Other (not defined)	2005	0

Suspicious transaction reports		
	Year (for 2007: to Sept only)	**Number**
	2006	20
	2007	37

Effectiveness (casinos, real estate and dealers in precious metals and stones)

630. Although these sectors are covered by the general duty to report STRs, the figures for reporting raise some concerns over the effectiveness of the provisions. The casinos and real estate agents spoken to were aware of the general duty to report in the circumstances where mandatory reporting is required, and also appeared to follow the fairly prescriptive criteria set out in Order 104 when considering whether a transaction was suspicious. The evaluation team was given figures for STRs by real estate agents for the past 3 years. Historically, these figures are low, especially in an economy where the purchase of real estate is growing. The figures for casinos are erratic, with a peak in 2006, followed by a drop in 2007. The evaluation team has concerns as to how comprehensive the overall regime is for real estate agents, given the reliance by the Russian authorities on information from several sources to trace the sale and purchase of real estate, and the possibility of cash being used to finance transactions.

631. The casinos and real estate agents spoken to had established internal systems and controls in compliance with the requirements of the AML/CFT Law, including appointment of a compliance officer, some form of internal audit, training and screening of employees. However, the historically low level of reporting in the real estate agent sector and the erratic figures for casinos, coupled with the lack of understanding of ID requirements in one casino visited raise concerns about current levels of effectiveness of these provisions.

632. In the absence of any countries on the NCCT list, the requirement for paying special attention to business relationships with persons from or in countries which insufficiently apply the FATF recommendations is not being met.

633. As the evaluation team did not meet with any dealers in precious metals and stones who are dealing in cash, effectiveness in this sector is difficult to determine. However, the figures for STRs cover some 25 000 firms, which include many that do not fall under the FATF definition (*e.g.* those not dealing in cash, and those involved in extraction of precious stones). The figures show a significant decrease in the number of STRs submitted. In the absence of a further breakdown of these figures, the effectiveness of the STR regime cannot be assessed.

634. More generally, although sanctions have reportedly been imposed in the casino and real estate sectors for failure to report to the FIU and for breaches of the internal control requirements, the lack of specific detail about the nature of these breaches and the penalties imposed means that effectiveness cannot be judged.

Effectiveness (lawyers, notaries and accountants)

635. The figures for submission of STRs by lawyers and notaries appear to be very low, which calls into question whether the requirements under the AML/CFT Law are sufficiently publicised, understood or enforced. It is clear that the SROs representing lawyers and notaries are aware of the need for their members to develop systems of internal control, but the lack of supervision for lawyers (and accountants) calls into question the effectiveness of the regime. In addition, although the Notary Chambers carry out supervision visits, the lack of identifiable sanctions linked to those visits raises doubts about effectiveness. In the absence of any definitive figures relating to reporting by

accountants, and in the absence of any meetings with the sector, the evaluation team was not able to judge the effectiveness of the provisions.

636. In the absence of any countries on the NCCT list, the requirement for paying special attention to business relationships with persons from or in countries which insufficiently apply the FATF recommendations is not being met.

Additional elements

637. The reporting requirement in the AML/CFT Law is not extended to additional activities of accountants.

4.2.2 Recommendations and Comments

638. Although all sectors of DNFBP (except TCSPs) are covered by the requirement to report STRs, the overall figures are inconclusive as far as effectiveness is concerned.

639. Russia should take steps to ensure that all institutions covered by the requirement to report STRs are aware of the difference between these reports and those relating to mandatory control.

640. Although sanctions have reportedly been imposed for breaches of the requirement to submit STRs and to have internal controls, there is a lack of information on precisely what the failings were. This information, if available, could be used to target areas where further guidance is needed.

641. For lawyers, notaries and accountants, Russia should take steps to improve understanding of the requirements in this area, given the current low level of reporting, and the lack of information available to evaluate the effectiveness of the regime.

642. The authorities should continue working with lawyers, notaries and accountants to ensure full compliance with the requirements relating to internal controls.

643. Russia should take further steps to ensure that covered institutions are aware of the need to pay special attention to customers from countries that do not sufficiently apply the FATF Recommendations.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**PC**	*Applying R.13* • Similar technical concerns to those recorded under Recommendation 13. • Casinos: Inconsistent levels of reporting lead to some doubts about effectiveness. • Real estate agents: Historically, relatively few STRs submitted. • Dealers in precious metals and stones: Large sector with relatively few STRs; lack of clarity as to how many STRs relate to the sector covered by the FATF definition. • Lawyers/notaries: Few STRs in this sector give rise to concerns over effectiveness. • Accountants – No specific information received. *Applying R.14* • Similar technical concerns to those recorded under Recommendation 14. *Applying R.15* • Casinos/real estate agents/dealers in precious metals and stones – similar technical concerns to those recorded under Recommendation 15, and overall doubts about effectiveness. • Lawyers/notaries/accountants – Doubts about effectiveness given the lack of

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
		AML/CFT supervision of lawyers and accountants and lack of information about supervision of notaries. Applying R.21 • No relevant requirements. • All Recommendations: TCSPs are not covered. • Accountants – no information on effectiveness.

4.3 Regulation, supervision and monitoring (R.24-25)

4.3.1 Description and Analysis

644. At the time of the on-site visits, the evaluation team was informed by various regional offices of Rosfinmonitoring that visits were targeted largely on the basis of the institution's turnover and the number of STRs submitted. Subsequent to the on-site visits, the Russian authorities provided the evaluators with details of a more sophisticated methodology, with an overall approach based on a risk assessment of institutions by the Supervisory department. For this, the FIU database of reported STRs and mandatory reports is searched by using algorithms. The output is a classification of businesses (no risk / high risk / serious problems / critical state). Since the total number of reports from supervised DNFBPs is relatively low when compared to the total number of DNFBPs, the output might reveal more high risk businesses than could effectively be targeted by supervisors on the ground. Although adherence to this approach was not apparent at the time of the on-site visits, a move towards a more risk-based approach to scheduling supervision visits is to be encouraged.

645. Under article 13 of the AML/CFT Law the General Prosecutor has a role in performing supervision over the AML/CFT Law. If violations are discovered, referrals are made to Rosfinmonitoring who is able to impose sanctions under article 15.27 of the Code of Administrative Offences.

646. Rosfinmonitoring co-ordinates its approach with the General Prosecutor and requests targeted inspections to be done by them. The assistance of the Prosecution Authority can be helpful in remote regions, where Rosfinmonitoring regional offices are not located. Discussions with representatives from the General Prosecutor's office during the on-site visits suggested that their powers were limited to checking whether the firm is registered and carrying out a quantitative check on whether the firm has internal control rules (including the requirement to submit STRs and carry out CDD), as opposed to a qualitative check of the appropriateness of the rules. Some time after the on-site visits Russia provided information which suggests that the role of the General Prosecutor's Office in supervision is more widespread, with them having the ability to carry out visits at the request of Rosfinmonitoring and to submit information for consideration of sanctions. Specimen disciplinary notices suggest that the supervision carried out includes a check on the completeness of identification information, the requirement to submit STRs and mandatory reports. The evaluation team was unable to determine what training was provided to the prosecutors to enable them to carry out their supervisory work.

Casinos

647. According to Order No. 183n, Rosfinmonitoring is responsible for monitoring compliance with the AML/CFT Law by casinos. Casinos are required to register with Rosfinmonitoring under Ordinance 28. This is a basic registration requirement, and casinos are additionally required to obtain a licence from Goskomsport (the State Sports Committee). The Goskomsport licence is a general business licence[132] and has no relation whatsoever with any AML/CFT requirement, except for the fact that it could be revoked for AML/CFT violations. This power has never been used (article 13, AML

[132] Paragraph 76, article 17 of Federal Law no. 128-FZ.

/CFT Law). In addition, there are no legal or regulatory requirements to prevent criminals or their associates from holding or being the beneficial owner or a significant controlling interest, holding a management function in, or being an operator of a casino. The Russian authorities consider that additional measures are contained in Order 104, which deal with internal controls for non-CIs covered by the main provisions of the AML/CFT Law. Appendix 7 requires the absence of a criminal record as one of the criteria for a compliance officer. However, this provision does not directly address the question of preventing criminals or their associates from holding a controlling interest in or managing a casino.

648. Rosfinmonitoring has the power to conduct on-site visits and to obtain documentation (Order 183n). These visits are undertaken by the central office and by the regional offices. Article 15.27 of the Code on Administrative offences of Russia sets a penalty of 100 to 200 times the minimum wage on officials for breaches of the AML/CFT Law, and a penalty of 500 to 5 000 times the minimum wage for similar breaches by legal persons. In addition, activities can be suspended for up to 90 days. This was the practice in two cases relating to casinos for AML/CFT violations. Rosfinmonitoring has the power to petition the existing licensing authorities to request the revocation of a business licence on the basis of article 13 of the AML/CFT Law quoted above. This has not been used in practice.

649. Rosfinmonitoring reported that it had conducted 241 on-site and 102 off-site casino inspections from 2003 to 2006. In addition 182 on-site casino inspections files were sent to Rosfinmonitoring from the General Prosecutor's Office. The evaluation team was told by the regional offices that visits are planned on the basis of turnover, and that although the risk in the casino sector is perceived as one of the higher risk areas supervised by Rosfinmonitoring, this did not lead to a greater resource concentration in this area. Feedback on STRs given to supervised institutions is limited to an acknowledgement of receipt. Additional guidance is given via the Rosfinmonitoring annual report, the website and in seminars, which supervised institutions were generally content with. In addition, most felt able to contact Rosfinmonitoring for guidance on specific issues.

650. Sanctions were imposed on 134 establishments and their directors from 2003 – 2006, and another 35 sanctions were imposed as a result of off-site inspections. Based on files received from the Prosecution Authority, another 116 sanctions have been imposed. The activities of two casinos have been temporarily frozen. The evaluation team requested a specific breakdown of sanctions imposed (both centrally and from the regional offices), but received only the above general information and an indication that the breaches related to organisation of internal control, fixing and reporting of information subject to mandatory control and identification of customers. In the absence of more specific information, the effectiveness of the regime is difficult to assess, but the lack of an effective sanctioning power enabling Rosfinmonitoring to directly withdraw a licence is a gap in the system.

Real estate agents

651. Real estate agents are required to register with Rosfinmonitoring under Order No. 183n. Rosfinmonitoring's powers to monitor, conduct visits and impose sanctions are the same as for casinos. Rosfinmonitoring carried out 12 visits to real estate agents in 2005 and 48 in 2006, and conducted 62 off-site inspections in 2006. In addition the Prosecutor General's Office conducted inspections on real estate agents and has sent 713 materials of inspections to Rosfinmonitoring in 2004-2006, as well as 402 in 2007.

652. Sanctions were imposed on five firms in 2005, 42 in 2006 and 185 in 2007. Prosecution Authority files resulted in another 436 sanctions between 2005 – 2006 The evaluation team asked for a specific breakdown of sanctions imposed (both centrally and from the regional offices) but only received the above general information and an indication that the main breaches related to organisation of internal control and identification of customers. In the absence of more specific information, the effectiveness of the regime is difficult to assess.

653. Feedback on STRs given to supervised institutions is limited to an acknowledgement of receipt. Additional guidance is given via the Rosfinmonitoring annual report, the website and in seminars, which supervised institutions were generally content with. In addition, most felt able to contact Rosfinmonitoring for guidance on specific issues.

Dealers in precious metals and stones

654. Dealers in precious metals and stones are required to register with the Assay Chamber under Order 91. The Assay Chamber supervises 25,000 firms, and carries out around 305 inspections per annum. It is not clear from the statistics provided to the evaluation team how many of these firms are technically captured by the FATF definition, as some firms are involved in extraction of precious stones, and some do not deal in cash. It is estimated that approximately 13 000 firms fall within the FATF definition. There are 18 inspectorates, and 20 to 30 inspections are carried out jointly with Rosfinmonitoring each year. The Assay Chamber's powers of supervision are carried out under Order 76n, and this includes the carrying out of inspection visits. Reports making recommendations are prepared, and ultimately the sanctions available under article 15.27 of the Code of Administrative Offences are available, but the power to impose these rests with Rosfinmonitoring. The Assay Chamber has a very wide-ranging set of responsibilities, including certification of precious metals and stones, and consumer protection. It has 3 supervisory staff in its Moscow office, and 75 in the 18 regional offices. However, the evaluation team was told that very few of these staff are AML/CFT specialists. At the same time the Assay Chamber is assisted both by Rosfinmonitoring (through targeted information provided on higher risk entities) and the General Prosecutor's Office, which also carries out inspections.

655. Supervisory visits involve a check of internal control rules, appointment of a compliance officer, record keeping, identification and submission of STRs. The evaluation team was informed that violations of each of these elements had been identified during on-site visits.

656. Feedback to supervised entities is given in seminars and in reports submitted after on-site visits. In addition, the Assay Chamber operates a helpline.

Effectiveness (casinos, real estate agents and dealers in precious metals and stones)

Casinos

657. The current system where casinos are not licensed by a competent authority which is involved with combating money laundering and terrorist financing is a matter of concern. Although the licence can technically be revoked based on non-compliance with the AML/CFT Law, this power has never been used. Supervision of casinos is conducted by Rosfinmonitoring, who also has responsibility for supervising all gambling institutions, as well as leasing companies, pawnshops and estate agents. Although some regional supervisors identified casinos as a high-risk area, this did not appear to be met with a proportionate allocation of supervisory activity. In the absence of specific information on sanctions imposed, doubts must remain as to the effectiveness of the regime. The authorities indicated that the assistance of prosecutors is most often used for remote regions, which are far away from the regional offices of Rosfinmonitoring. In those cases Rosfinmonitoring usually sends targeted requests to the prosecutors to check a certain entity. Some of the regional offices met did not have full staffing levels, at the time of the on-site visit, and the evaluation team was informed that this was because of the exacting requirements for hiring new employees. It is understood that these vacancies had been filled by April 2008.

Real estate agents

658. The evaluation team was surprised to meet with a regional office of Rosfinmonitoring whose representative expressed some doubt over whether real estate agents were within the scope of their supervision. The Russian authorities thought this was due to interpretation difficulties. Different

figures have been provided to the evaluation team for on-site inspections and sanctions imposed on this sector, and there are inconsistent figures for the number of estate agents. The Russian authorities report that number of estate agents has risen from 1 859 at the beginning of 2007 to 3 285 at the end. Current figures suggest that Rosfinmonitoring carried out a mixture of on-site and off-site inspections totalling 122 from 2004 to 2006. The Prosecutor's office submitted 713 files from 2004 to 2006. Current figures suggest that 484 sanctions were applied from 2004 to 2006. Again, in the absence of a fuller breakdown, it is difficult to judge the effectiveness of the supervisory and sanctioning regime. The evaluation team continues to have doubts as to the overall strategy involved with identifying, registering, monitoring and sanctioning real estate agents, not least because of the variety of figures provided and the wide range of agencies involved in dealing with all aspects of their work.

Dealers in precious metals and stones

659. The evaluation team was informed by one of the bodies met that in the Russian context, the absence of a licensing regime (instead of the current registration system) for dealers in precious metals and stones is a factor that reduces the effectiveness of the supervisory regime carried out by the Assay Chamber for dealers in precious metals and stones was a factor in reducing the effectiveness of the supervisory regime carried out by the Assay Chamber. The lack of effective AML/CFT supervision and AML/CFT devoted resources is overwhelming. The Assay Chamber has a very large population (25 000 dealers, of which it is estimated that 13 000 are covered by the FATF definition) and a limited number of staff, very few of whom are AML/CFT specialists. For example, the Far Eastern district has one AML/CFT specialist responsible for several hundred firms, and the Rostov-on-Don district has two AML/CFT specialists responsible for 811 firms. At the same time the Assay Chamber is assisted both by Rosfinmonitoring (through targeted information provided on higher risk entities) and the General Prosecutor's Office, which also carries out inspections. The Assay Chamber's responsibilities are far wider than those relating to AML/CFT. Given the situation in Russia, where all aspects of the process, from extraction through to sale, are dealt with, additional and more specialist resource would increase the scope and depth of supervisory visits. For example, one regional office suggested that jewellery dealers posed higher AML/CFT risks.

660. Supervision largely consists of examining written internal control procedures submitted by institutions, with a limited number of on-site visits, which follow a planned visit programme agreed with the central office. One regional office indicated that access to the content of STRs submitted by its firms would be a useful supervisory tool. The Assay Chamber does not have power to impose sanctions on the firms it supervises, but makes recommendations to Rosfinmonitoring, who are able to impose financial penalties. A total of 147 sanctions were imposed in 2005 and 2006, the majority of which related to issues of internal control. In the absence of a detailed breakdown, effectiveness is difficult to judge. Previously submitted figures suggest that from 2003 to 2006 Rosfinmonitoring received 412 inspection files carried out by the Assay Chamber and the General Prosecutor's Office. This resulted in a total of 197 sanctions. In the absence of further information about the nature of the breaches and the sanctions imposed, it is difficult to judge effectiveness.

Lawyers, notaries and accountants

661. The main supervisory body for the general activity of lawyers is the Russian Registration Committee in the MoJ. However, this has no supervisory control for AML/CFT purposes. In addition, the Federal Lawyers' Chamber and the regional Lawyers' Chambers have general professional conduct responsibility for the approximately 60 000 lawyers practising in Russia. Lawyers must register with one of the chambers to be able to represent clients in court. Regional chambers are able to carry out inspections of lawyers' firms, although these powers have not been utilised in checking compliance with the AML/CFT Law. In April of each year lawyers are required to submit a copy of their financial accounts to the relevant regional chamber. The evaluation team was told that the Council of the Federal Lawyers' Chamber regularly discusses AML/CFT issues, and that the results of these discussions are publicised. Other than this, the evaluation team was given no details of feedback given to members.

662. The Notary Code requires all notaries to be members of a regional Notary Chamber. These chambers carry out visits once a year, and in the past four years all notaries have been visited. These visits include general checks on whether the notary has internal controls for AML/CFT. General powers available for monitoring appear to be adequate, but in the absence of information about sanctions for AML/CFT breaches, powers of sanctioning must be in doubt.

663. The evaluation team was not given the opportunity to meet with any representatives from either the accountancy profession or its supervisor during the on-site visits. Information provided by the Russian authorities some time after the evaluation indicated that the designated authority for accountants is the MoF in accordance with article 14 of the Auditing Law. The MoF may perform its own inspections or delegate this authority to professional auditor associations accredited by the MoF who then inspect compliance of their own members. The sanctions imposed on accountants can include the withdrawal of the licence, although it is understood that this has not been imposed for breach of AML/CFT rules. As accountants fall under the AML/CFT Law their compliance with the Law is reportedly checked in the course of inspections. Figures provided by the Ministry of Finance suggest that 515 inspections of accounting firms were carried out in 2006, with a further 577 in 2007. In addition AML/CFT requirements are included in the Code of Ethics of auditors, and compliance with this code of ethics is checked.

Effectiveness (lawyers, notaries and accountants)

664. The supervision of lawyers concentrates on matters relating to professional practice and observance of federal legislation, including, in theory, AML/CFT. It is thus difficult for Russia to demonstrate that the regime is effective. Notaries are subject to a more detailed supervisory regime, with all firms having been visited for professional practice purposes over the past four years. However, the absence of linked sanctions relating specifically to AML/CFT or follow-up action to those visits brings the effectiveness of the regime into question.

665. The evaluation team was not given the opportunity to meet with any firms or supervisory staff during the on-site visits, and no specific information about sanctions has been provided.

4.3.2 Recommendations and Comments

666. The current supervisory regime is somewhat fragmented, with a variety of supervisors having responsibility for a diverse range of firms. This in itself is not a ground for criticism, but in order to demonstrate that it has an effective regime, Russia should improve the data available to analyse the effectiveness of the measures it is taking. A systematic review of the feedback given to supervised institutions would ensure that there is a consistent understanding of the requirements of the AML/CFT Law.

667. Rosfinmonitoring should consider introducing a greater element of risk-based supervision in relation to the categories of firms it supervises. In particular, the risks identified by Rosfinmonitoring in relation to casinos should be subject to greater supervisory attention.

668. The role of real estate agents should be examined to ensure that no gaps exist in the AML/CFT system. In particular, the contention that most flows of funds in real estate transactions are routed through the banking sector should be verified, and the level of risk relative to the supervisory activity of Rosfinmonitoring in this area should be considered.

669. The system for supervising lawyers' and notaries' compliance with the AML/CFT Law is rather limited. The effectiveness of the regime for notaries would be better demonstrated if figures for sanctions related to AML/CFT breaches were available.

670. The current regime for licensing casinos will not change until 30 June 2009 (see section 1). In the meantime Russia should consider how it will implement this change and develop plans to deal

with unlicensed gambling. The current and future regime contains no specific provision to prevent criminals or their associates from holding an interest in a casino. This should be addressed.

671. The Assay Chamber should have more specialist AML/CFT staff in order to better perform its functions.

672. Consideration should also be given to the Assay Chamber's suggestion that supervisors be given greater access to the content of STRs in order to better target supervisory action.

673. Russia should take further steps to strengthen the AML/CFT supervisory regime for accountants.

4.3.3 Compliance with Recommendations 24 & 25 (criteria 25.1, DNFBP)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	**PC**	• No current AML/CFT licensing regime by an AML/CFT competent authority for casinos. • No measures to prevent criminals holding an interest in a casino. • Limited number of focused supervisory visits to real estate agents. • As reported on-site, supervisory activity for casinos does not appear to be proportionate to the perceived risks identified by the supervisor. • Monitoring of lawyers is remote and not specific to AML/CFT. • No details of specific AML/CFT monitoring of notaries. • Assay Chamber does not consider itself to have adequate powers. • Assay Chamber has relatively few AML/CFT specialists to supervise 25 000 firms. • General lack of specific information to assess effectiveness of the sanctions regime relating to DNFBPs. • TCSPs not covered.
R.25	**PC**	• Limited feedback given to the dealers in precious metals and stones, lawyers and notaries. • No information about feedback given to accountants.

4.4 Other non-financial businesses and professions / Modern secure transaction techniques (R.20)

4.4.1 Description and Analysis

Other non-financial businesses and professions

674. Russia has considered applying Recommendations 5, 6, 8 – 11, 13 – 15, 17 and 21 to other non-financial businesses and as a result has designated pawnshops, operational leasing companies and non-casino gambling enterprises. As a result, all the measures described in section 3 (financial institutions) and sections 4.1 to 4.3 (DNFBPs) apply to these sectors.

Modern secure transaction techniques

675. The Russian economy remains predominately cash-based, which is not surprising given its history of severe banking crises in the 1990s. The Russian government has identified as a key policy objective the creation of a structurally sound, reliable, and effective banking system to support economic growth; however, such a development would also reduce Russia's vulnerability to basic cash-based ML and TF. The policy objectives set out in the BoR's Strategic Banking Development Paper establishes a deadline of 2008 to accomplish a series of key objectives to reduce the Russian economy's reliance on cash-based transactions. Item 5 of the Paper seeks to improve public confidence in the banking sector sufficiently to encourage the public to move its accumulation of cash

from "under the mattress" to credit institutions, thus reducing the amount of cash circulating in the economy.[133] Item 8 of the Paper calls for the creation of legal conditions to support the use of modern electronic technologies in the banking sector.

676. The measures to promote modern and secure techniques and the restrictive measures for cash-based transactions have led to an increase in non-cash settlements in Russia over the last years. Over the years 2005 – 2007, the number of non-cash settlements has doubled, and the total value of such settlements has more than doubled. The number of bank cards issued has also doubled during this time frame, while the use of such cards has tripled.

677. The highest denomination bank note in Russia is RUB 5 000, with the second highest RUB 1 000.

4.4.2 Recommendations and Comments

678. Russia is to be commended for identifying pawnshops, operational leasing companies and non-casino gambling enterprises as designated entities under the AML/CFT Law. Russia may also want to consider the ML risk posed by the proliferation of high value and luxury goods providers in Moscow and other major urban centres that has accompanied Russia's recent oil boom.

679. Russia should seek to continue reducing its reliance on cash and introduce more efficient payment systems that have also been introduced in other countries around the world. Adopting more modern payment techniques should also reduce the need for high denomination bank notes. The RUB 5 000 bank note represents more than twice the current minimum monthly wage of RUB 2 300.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**C**	• This Recommendation is fully observed.

5. LEGAL PERSONS AND ARRANGEMENTS & NON-PROFIT ORGANISATIONS

5.1 Legal Persons – Access to beneficial ownership and control information (R.33)

5.1.1 Description and Analysis

680. All legal entities and individual businesses are required to register or update their registration at the moment of their establishment, reorganisation and liquidation as well as when any changes to the constituent documents are introduced. The law describes the data that have to be submitted to the registry (the Unified State Register of Legal Entities, USRLE) – which is maintained by the FTS. Information is publicly available, except for certain types of information that is only available to the state authorities. Information on beneficial ownership and control of legal persons according to the requirements of the FATF Recommendations is not registered or readily available to any state authorities.

Registration

681. The following legal entities are required to register with the USRLE. See section 1 of this report for an introduction to the different legal entities in Russia.

[133] Government Statement no. 983p-P13, BoR Letter no. 01-01/1617 of 05.04.2005 "On the strategy of development of the banking sector of Russia for the period until 2008".

682. Commercial entities: limited liability partnerships, limited liability companies, limited partnerships, double limited companies, joint stock companies, production co-operatives and state-run and municipal unitary enterprises.

683. Non-profit entities: consumer co-operatives, public and religious organisations and associations, funds (charity), institutions and associations and unions of legal entities (non-profit entities are further discussed in section 5.3 of this report).

684. All legal entities are required to provide data to the USRLE[134]. The USRLE is maintained by the FTS and records are entered into the system on the basis of information provided by the legal entity. Registration is compulsory, without it the legal entity is not considered to exist. The following data and documents are required by the USRLE:

- Full name of the entity, abbreviated name, firm name for commercial organisations, all in Russian and in its original language.
- Legal form.
- Mailing address of the permanent executive body of the legal entity – or – another body or person entitled to act on behalf of the legal entity (communication channel, without any power of attorney).
- Method of incorporation of the legal entity (newly created or based on existing legal entities).
- Information on founders (members) of the legal entity, in case of joint stock companies also information on those who hold shareholders registers (if applicable).
- Original or notarised copies of the constituting documents of the legal entity.
- Information on legal succession and history (predecessor entities or amendments, also for legal entities that have merged into other legal entities or have otherwise been reorganised).
- Date of registration of any amendments.
- Information on manner of liquidation of the legal entity, or information on the fact that it is being liquidated.
- The size of the authorised capital stock (charter capital, authorised fund, share contributions or other) specified in the constitutive documents of the commercial organisation.
- Family name, first name, patronymic, position, passport data (or equal) and taxpayer identification number of the person entitled to act on behalf of the legal entity without any power of attorney.
- Information on licences obtained by the legal entity.
- Information on branches and representative offices of the legal entity.
- Taxpayer identification number, code of the reason for and date of registration of the legal entity at a tax authority.
- Codes according to the all-Russian classifier of types of economic activity.
- Number and date of registration of an insurer (for pension, compulsory medical insurance and social security purposes).
- Information on bank accounts of the legal entity.

[134] Federal Law of 08.08.2001 N 129-FZ "On state registration of legal entities and individual entrepreneurs".

685. All information in the USRLE is publicly available, except for banking and personal information[135]. Banking and personal information is, however, available to state authorities, including law enforcement bodies and courts (for legal cases), local authorities, bodies of state extra budgetary funds and persons determined by federal law and regulation. In return, all these bodies can submit information to the USRLE, except for information on the private life of citizens. Finally, based on the AML/CFT Law, the tax authorities must provide Rosfinmonitoring with all information contained in the USRLE, if it concerns any of the designated reporting entities under the AML/CFT Law (article 5) and any other information Rosfinmonitoring needs to perform its tasks.

Beneficial ownership

686. Beneficial ownership (BO) as defined in the FATF Recommendations is not registered in the USRLE, nor is BO information required to be retained by legal entities. There is also no explicit requirement for FIs or DNFBPs to identify the beneficial owners of legal persons.

Bearer shares

687. Pursuant to article 145 item 1 Civil Code, the rights, certified by a security, may belong to the bearer of the security, but item 2 stipulates that a law may preclude the possibility of issuing a certain kind of security as those to bearer. The Securities Law defines a security (or share) as any paper security, including a non-documentary security that records the totality of property and non-property rights subject to certification, assignment, and unconditional exercise. The law equally defines that bearer shares (or "securities issued to bearer") are securities, the transfer of rights to which, and the exercise of the rights recorded by which, do not require the identification of the owner (article 2).

688. In accordance with article 25 of Federal Law No. 208-FZ dated December 26. 1995 "On joint-stock companies" all shares of a joint stock company are nominal. The evaluation team was assured by the Russian authorities that thus, the possibility of issuing bearer shares is precluded and that bearer shares have never been issued in Russia. The evaluation team does not have any indications that this is not true.

Additional elements

689. Russia has taken no measures to facilitate access by FIs to BO information. On the contrary, the little information on the beneficiaries that is available to the authorities is collected by FIs themselves, and is not available for other FIs.

Effectiveness

690. According to the Russian authorities, the overwhelming majority of money laundering methods are associated to a certain extent with "one day" firms – commercial organisations registered as fake persons without intention to perform any real commercial activity. The evaluators believe that an important reason for this is the lack of information on beneficial ownership and control of legal persons that meets the requirements of the FATF Recommendations. The evaluators strongly believe that if there were effective procedures in place to establish such information, the problem with the "one day" firms would be resolved to a large extent.

5.1.2 Recommendations and Comments

691. The Russian authorities should implement a system that requires adequate transparency regarding the beneficial ownership and control of legal persons.

[135] Clause 1 article 6 of Federal Law no. 129-FZ.

5.1.3 Compliance with Recommendation 33

	Rating	Summary of factors underlying rating
R.33	**PC**	• None of the existing systems achieve adequate transparency regarding the beneficial ownership and control of legal persons.

5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)

5.2.1 Description and Analysis

692. The Russian legal system does not allow for the creation of trusts, and the legal concept of trust does not exist under Russian law. Russia has not ratified the 1985 *Hague Convention on the Law Applicable to Trusts and on their Recognition*.

693. The concept of "fiduciary management" exists in Russia, but this differs from the traditional legal concept of trusts as property rights are not ceded to the fiduciary manager. Those who carry out fiduciary management responsibilities must obtain a licence as participants in the equity market and are therefore subject to the provisions of the AML/CFT Law.

5.2.2 Recommendations and Comments

694. Recommendation 34 is not applicable in Russia.

5.2.3 Compliance with Recommendation 34

	Rating	Summary of factors underlying rating
R.34	**N/A**	• This recommendation is not applicable.

5.3 Non-profit organisations (SR.VIII)

5.3.1 Description and Analysis

Review of the NPO sector

695. The current law that regulates all non-profit organisations in Russia, the Non-profit Organisations Law[136] (NPOL), dates back to 1996. Since enactment it was updated in 1998, 1999, 2002 (2x), 2003 and 2006 (5x). The Russian authorities did not indicate if these amendments are minor technical changes or extensive changes. Some time after the on-site visits, the Russian authorities provided the evaluation team with a review document of the non-profit sector, which had been drafted in 2007. It is unclear what sources were used, what information was collected and how long it took to obtain the necessary information. Nevertheless, the evaluation team concluded that the Russian authorities have undertaken a review of the NPO sector, albeit a superficial one.

Outreach

696. The Russian government has undertaken some outreach towards the NPO sector. For example, Rosfinmonitoring has organised conferences and seminars for NPOs, with the involvement of other competent authorities. This has also been done as part of Council of Europe capacity building assistance (Moli-Ru). The specialised monthly magazine "Non-profit organisations in Russia" also covers matters related to NPOs and terrorist financing, accounting, reporting and taxes.

[136] Federal Law no. 7-FZ on non-profit organisations.

697. Although the information on the website of Rosfinmonitoring targets a broad audience and Rosfinmonitoring publishes annually articles about AML/CFT, also in relation to NPOs (the evaluation team did not receive examples), the evaluation team is under the impression that none of the competent authorities feels any specific responsibility in relation to outreach and guidance to the NPO sector.

Available information

698. Information on the purpose and objectives of their stated activities is included in the charter of the NPO. A charter includes information on the name of the non-profit organisation, the nature of its activity, form of incorporation, address of the NPO, management procedure, subject and objectives of activity, information about branches and representative offices, rights and obligations of members, conditions and procedure for acceptance of members of the NPO and withdrawal from it (if the NPO has membership), sources of financing of property of the NPO, procedure for introduction of amendments into the constitutive documents of the NPO, and the procedure for use of property in case of liquidation of the NPO. (NPOL, item 3, article 14).

699. The charter documents of the NPO (the constituent documents, amendments and data on founders) presented to ROSREG (or its territorial bodies) for the purpose of state registration are sent to the registration body (FTS) for entering into the USRLE. USRLE contains, among other things, the following data and documents of an NPO: the full and abbreviated name; the legal form; the address of a permanent executive body; the way of formation; data on founders; data on assignment; the date of registration of changes into charter documents; the (sur)name, passport data and job position of the person with power of representation; data of licences of the NPO; data on affiliates and representations; the taxpayer identification number and bank account data. All this information is publicly available, except for bank and private data. All information is accessible to state authorities. These data have to be submitted to ROSREG within three months. As of December 2007, 228 179 NPOs had registered with ROSREG.

700. On the basis of the NPOL, NPOs are obliged to present to ROSREG the documentation containing reports on its activity, personnel of management bodies, as well as documents on expenditure of monetary funds and on the usage of other property including resources received from international and foreign organisations, foreign citizens or persons without citizenship (NPOL, article 32). The reporting forms and terms are determined by the government[137].

701. At the end of 2007, ROSREG had received 49 211 such reports of NPOs, which is only about 22% of 228 179 registered NPOs[138].

702. The legislation does not establish the requirement on annual publication of reports on use of property to all forms of non-profit organisations.

703. Foreign NPOs ("structural subdivision of the foreign non-profit non-governmental organisation") have to disclose to ROSREG the amount of property and funds it possesses. Foreign NPOs also have to indicate how they intend to spend the funds and property and how the funds and property have actually been used and if all this is in line with the terms set by the Russian government.

Sanctions

704. Violation of the law or actions contradicting the purposes stated in the charter can lead to a sanction. In case of a minor wrongdoing, ROSREG can issue a written warning and demand that the situation be corrected within a month.

---

137 Ordinance no. 212 of 15.04.2006 in the version of Ordinance no. 213 of 10.04.2007.

138 This includes 90 708 trade unions and 1 158 political parties that do not have to submit reports.

705. Repeated failure of a domestic NPO to submit within a set timeframe activity documents, information on staff, documents on spending of monetary funds and use of other property including those received from international and foreign organisations, foreign citizens and stateless persons, will lead to an application of ROSREG to court for liquidation of the NPO (NPOL, articles 32.4 and 32.10). The authorities indicated that in 2007, of the 6 260 liquidated legal entities, 25 entities have been liquidated because of terrorist activity.

706. If a branch of a foreign NPO fails to meet the legal requirement, ROSREG may issue a warning and has the right to apply to court for liquidation of that branch. The norms for creation and liquidation of a branch of a foreign NPO are equal to the norms that apply to domestic NPOs. A separate procedure for creation and liquidation has been established for affiliates and representative offices of foreign NPOs (as they are not legal entities in Russia). ROSREG may issue a warning and directly exclude it from the register, without a need for a court order (NPOL, item 8, article 32). In 2007, 34 warnings had been issued to affiliates and representative offices of foreign NPOs.

707. If the constitutional order, morality, health, rights and legal interests of other persons, defence and safety of the state are under threat, ROSREG may inform the foreign NPO that a particular transfer of funds or property, or the transfer of funds or property to a certain entity, is prohibited.

708. ROSREG has the right to pass a written prohibition of transfer of monetary funds and other property to specified recipients of the indicated funds and property to the branch of a foreign non-profit non-governmental organisation. Up until now ROSREG has not taken any decision on prohibition of transfer of funds or other property.

709. In 2007, ROSREG issued around 44 000 written warnings to NPOs for violations of the legislation. The two main violations were non-advising ROSREG on changing of the address and non-presenting of reports.

Licensing and registration

710. All legal entities are registered in Russia, see sections 1 and 5.1 of this report for details. There are different organisations involved in control over the activity of NPOs:

- Federal bodies of the state financial control.
- Federal Tax Service.
- Rosfinmonitoring.
- MIA.

711. Besides the above mentioned organisations ROSREG monitors whether the activity of an NPO is in accordance with the purposes stipulated in its constituent documents as well as over implementation of the legislation. ROSREG has the right to request administrative documents from the management bodies of NPOs. They can also request financial and economic information from other state authorities (state statistical institutions, tax authorities, other state supervisors) and from credit institutions and other FIs. ROSREG can perform annual checks of compliance of the activity of the NPO. These checks can be scheduled and non-scheduled and can be carried out on-site as well as through a review of documents. In 2007, ROSREG and its regional offices carried out 13 485 scheduled and non-scheduled checks. In case there is any suspicion of an offence or of terrorism, ROSREG performs more than one check per year[139]. MIA also does inspections, and in investigations involving suspicions of TF, MIA can and has used special investigative powers, such as undercover

[139] Regulation of ROSREG approved by order of the MoJ no. 380 of 25.12.2006, item 8, part 7.

operation and wire tapping. Rosfinmonitoring provides additional information to these investigations (financial analysis reports).

712. In ROSREG and its territorial bodies, 1272 persons are employed, but it is not quite clear how targeting NPOs is planned, except for the fact that other government bodies and concerned citizens may trigger a check.

Record keeping

713. The Russian authorities indicated that NPOs are required to account in accordance with the procedure established by the Russian government, and that NPOs have to provide information concerning financial planning and activities to competent authorities (see also below).

Information gathering to target abuse

714. Apart from the information gathered for the USRLE, the NPOL also obliges NPOs to present ROSREG with reports on its activity, personnel, management as well as documents on expenditure and usage of other property including resources received from international and foreign organisations, foreign citizens or individuals without citizenship. Templates and timing for reporting are defined by the government (NPOL, item 3, article 32).

715. The templates[140] for reporting were set in 2006. There are in total six templates, requiring NPOs to submit a great variety of information, such as a report on the activities of the NPO (excluding religious organisations), information on personnel of its management bodies, documents containing information on expenditures of monetary funds and usage of other property including funds and property received from international and foreign organisations and citizens and individuals without citizenship. In addition NPOs (including subunits) have to indicate their funds, forecast their spending, account for past spending, account for gifts received. Religious organisations need to submit information on the leadership and management of the organisation, its gifts and spending, in detail if received from foreigners or from abroad.

716. All the above information is kept by ROSREG. The reports indicate that in 2006, 1 155 NPOs received funds from international and foreign organisations, foreign citizens and individuals without citizenship.

Domestic co-operation to target abuse

717. In order to enhance domestic co-operation to target abuse of NPOs by potential terrorist financiers, the Interagency Commission for ML and TF has been tasked to resolve issues associated with operational interaction in the area of combating ML and FT, in particular in matters associated with prevention of use of NPOs for TF. ROSREG and Rosfinmonitoring claim to have developed and are agreeing upon a draft agreement on information sharing and interaction in the areas of NPOs. Rosfinmonitoring has provided ROSREG the list of organisations and physical persons in relation to which there is a suspicion of participation in extremist activity (as described in section 2.4 of this report).

Access and sharing information to target abuse

718. In 2007, MIA described approximately 10 cases that they investigated. In these cases (covering 25 regions) some NPOs were found to be related to TF. The operational activities were carried out in combination with the FSB and Rosfinmonitoring. The case descriptions were provided to other law enforcement bodies. The evaluation team could not determine whether there is one central authority that is aiming at national co-operation and the sharing of information. Rosfinmonitoring

[140] Government Decision no. 212 of 15.04.2006 «On measures for implementation of statements of number of Federal Laws regulating activities of non-profit organisation".

claims to be the appropriate point of contact for international requests for information. There was no state-level decision provided to the evaluation team that Rosfinmonitoring is the central authority responsible for NPOs.

5.3.2 Recommendations and Comments

719. The Russian authorities have undertaken a superficial review of the NPO sector with an aim to determine its vulnerability to terrorist financing. The evaluators urge the authorities to undertake a comprehensive review of the system, as foreseen by Special Recommendation VIII.

720. While the Russian authorities seem to be of the view that the system in place is quite tough, most of the provisions are basic registration provisions that are in place for all legal entities in Russia, also for commercial legal entities. While NPOs have up to three months to submit their data, it is unclear how long it takes ROSREG to check the data (if at all). Data are shared with Rosfinmonitoring, but the FIU has no insight as to the accuracy of the data. The new provisions that relate to reporting of NPOs to ROSREG could make a difference, however, these are not fully obeyed by the sector and not sufficiently enforced by the authorities.

721. There is some outreach to the NPO sector to provide guidance. All the work was done with a view to create a legal framework to control the NPO sector and to explain what rules are in place. This has little to do with outreach, as defined by Special Recommendation VIII. The authorities are urged to engage with the sector, to learn from the sector, to promote values and the like.

722. Lastly, the Russian authorities should set up a more formalised and efficient system that focuses on potential vulnerabilities and to share information to target abuse.

5.3.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**PC**	• The lack of a comprehensive review of the system means that not all the necessary measures have been taken and it is unclear what measures are part of a comprehensive policy to fight the misuse of NPOs by terrorist financiers, and what the effect of those measures has been (effectiveness issue). • Some of the rules are insufficiently enforced. • There is inconsistent outreach to the NPO sector to provide guidance. • There is no formalised and efficient system in place that focuses on potential vulnerabilities. • There is no formalised and efficient system in place to share information to target abuse. • No single authority is formally designated as the competent authority responsible for co-ordinating Russia's domestic efforts regarding NPOs and receiving international requests.

6. NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and co-ordination (R.31 & R.32)

6.1.1 Description and Analysis

Policy-level co-operation and co-ordination mechanisms

723. Policy-level co-ordination is organised top-down (President – Prime Minister – Rosfinmonitoring), with Rosfinmonitoring being responsible for co-ordination among other federal

ministries and executive agencies. The co-ordination framework and its objectives are laid down in the NASP (see section 1 of this report), and the action plan for implementation of the NASP for the period until 2010 has been approved.

724. Within the government, the Inter Agency Commission (IAC) is the standing co-ordinating authority. Its members[141] are represented at the director-level or deputy director-level and the Commission is chaired by the Head of Rosfinmonitoring. The tasks and duties of the IAC are:

- Preparation of proposals for implementation of the NASP.
- Ensuring policy and operational co-operation among federal executive bodies and the BoR.
- Inviting representatives of other executive bodies as necessary.
- Development of an international co-operation policy.
- Preparation of proposals to improve the AML/CFT system.
- Setting up working groups under the auspices of the IAC.
- Organisation of typologies-related work.
- Propose better information sharing policies and agreements, including with non IAC-members.
- Monitoring the progress of the IAC's work.

725. In accordance with its plan of work the IAC meets every two months. Besides, extraordinary meetings of the Commission may take place at the initiative of interested federal executive bodies or the BoR upon decision of the Chairman of the IAC (three such meetings took place in 2006-2007).

726. The IAC has set up three IAC working groups to address: *i)* legal and regulatory issues, *ii)* domestic operational inter-action, and *iii)* international co-operation. Since the IAC was established in 2005, seven regional IAC have been established, one in each Federal District, consisting of representatives from regional offices of Rosfinmonitoring, law enforcement and supervisory bodies. The objective of these IACs is to improve regional operational co-ordination and co-operation (prevention, investigations, specific AML/CFT cases).

727. The management of the FIU also helps to ensure broad inter-agency co-operation on the policy level by participating in other co-operating bodies, such as the National Anti-Terrorist Committee; the Interagency Commission of the Security Council for Social Security; the Annual interagency meeting of law enforcement and supervisory authorities with regard to AML/CFT matters; the Governmental Commission for combating the abuse of drugs and illegal turnover thereof; the Interagency working group on combating economic crimes and its working groups to combat offences in economic sphere; and the Commission for export control.

728. (Policy) co-ordination among law enforcement agencies is entrusted to the Prosecution Authority[142]. Co-ordinating meetings of law enforcement bodies (including on ML/TF issues) are regularly held by the Prosecutor General.

Effectiveness of inter-agency co-operation

729. Even though many agencies participate in formal AML/CFT inter-agency structures, most policy inter-agency co-operation naturally depends on Rosfinmonitoring, the BoR and the Prosecution Authority due to their central co-ordinating role in the AML/CFT system. During the meetings, the

[141] MoF, MIA, MFA, MoJ, the External Intelligence Service of Russia, FSB, FSKN, FFMS, the Federal Penitentiary Service, FCS, FISS, Rosfinmonitoring and BoR. The Prosecution may attend.

[142] Federal Law "On the Prosecution Bodies" and Presidential Decree no. 567 of 18.04.1996.

evaluation team did request other government bodies to state their policy views in relation to the AML/CFT system. In most cases, these bodies indicated that the implementation of the AML/CFT Law in their sector would be the priority (which should indeed be the case for some sectors). However, there was less appetite to indicate what other measures would be necessary to further improve Russia's AML/CFT system. For the further development of Russia's AML/CFT system, it is however pivotal the other agencies develop and articulate a policy view on these issues.

730. Operational co-operation among law enforcement bodies takes place through operational investigative groups, in which officers from all relevant law enforcement bodies can participate (MIA, FSB, Prosecution Authority, FSKN), based on the needs of each case (usually, of course, for significant cases). To establish a group, a legal order is needed from each of the participating groups. The evaluation team did come across some problems with operational inter-agency co-operation. In all visited regions, the Prosecution Authority representatives were not aware of the existence of particular ML/TF cases, despites its overall co-ordination authority. Law enforcement bodies also had some problems giving examples of joint investigation teams, even though the team met with law enforcement bodies that would typically be day-to-day counterparts in a region or city. That said, Russia did supply the team with examples of legal orders to form joint ML/TF teams after the on-sites.

Review of the effectiveness of AML/CFT systems

731. Russia appears to have mechanisms in place to review the effectiveness of its AML/CFT system, since new policy and legislative proposals are developed and implemented on an ongoing basis. Russia does not have a formal mechanism in place (outside general accountability reports), but the evaluation team considers the papers described in Section 1 (such as the NASP) to be sufficient proof of implementation. However, the evaluation team also notes that the valuable findings of reports such as the NASP and policy oriented typologies reports by Rosfinmonitoring, sometimes have a rather limited effect in areas that are outside the control of Rosfinmonitoring, such as compliance with Recommendation 33 and Special Recommendations III and IX. While Rosfinmonitoring already has the overall responsibility for the implementation of the FATF (Special) Recommendations, the evaluation team would recommend that Rosfinmonitoring should also be given the necessary corresponding powers to be able to ensure improved implementation.

Operational-level co-operation and co-ordination mechanisms

732. At present Rosfinmonitoring has signed 36 agreements of bilateral co-operation with federal executive bodies, BoR and self – regulated organisations (a full list of agreements was not provided).

733. Based on interviews with representatives from various law enforcement agencies, supervisors, and policy making bodies, the evaluation team concluded that operational-level co-operation and co-ordination to address the threat of illegal alternative remittance systems is wholly lacking. While the FIU and other supervisory bodies asserted that law enforcement and prosecutorial authorities are responsible for investigating crimes associated with illegal ARS, no law enforcement agency identified this as an area of concern and few, if any, resources are devoted to ARS.

Additional elements

734. In January 2007, the IAC established the Private Sector Consultation Committee. This Committee meets at least every two months and includes representatives of the banking sector, securities, insurance, gaming, lawyers, notaries and pawnshops.

735. Private sector representatives from various financial institutions reported close co-operation with the FIU and other supervisory bodies, such as the BoR. Both the FIU and the BoR have developed comprehensive training programmes for the private sector, and it appears that the private sector is strongly encouraged (and possibly even required) to partake in these training opportunities. Further, the requirement that the FIU and the Central Bank approve all internal control programmes

fosters a necessary dialogue between the private sector and the supervisors that appears to bolster Russia's overall AML/CFT regime.

Resources, professional standards and training (Recommendation 30)

736. Many AML/CFT policies are drafted at the level of the FIU, as was already discussed in section 2.5 of this report (which also included a discussion of the FIU's resources, professional staff and training). Beyond the data provided about the resource allocation of the FIU, the Russian authorities did not provide detail on the allocation of other resources used to set up and maintain the AML/CFT system on the policy level, except that the resources allocated were substantial. Likewise, no information was provided on AML/CFT training for non-FIU policy staff. Professional standards requirements are the same for both FIU staff and other government officials involved in AML/CFT.

6.1.2 Recommendations and Comments

737. The valuable outcome of policy reviews, such as the NASP and policy orientated typologies reports by Rosfinmonitoring (see section 1.5) are not always implemented as they should be, especially in areas that are not the responsibility of Rosfinmonitoring.

738. Russia should make an extra effort to enhance operational-level co-operation among law enforcement agencies, and between law enforcement and supervisory authorities to sharpen Russia's focus on the possible existence of illegal alternative remittance systems within Russia. This effort should aim to develop a sense of the threat as well as a prescription for addressing the problem.

6.1.3 Compliance with Recommendation 31

	Rating	Summary of factors underlying rating
R.31	**LC**	• Law enforcement agencies and supervisors do not adequately co-operate on the operational-level with respect to potential systemic vulnerabilities such as illegal money and value transfer services.

6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)

6.2.1 Description and Analysis

739. The Union of Soviet Socialist Republics ratified the Vienna Convention on 9 October 1990, and it came into force on 17 April 1991 (Russia is the successor state to the Union of Soviet Socialist Republics). All of the relevant articles of this Convention have been implemented by Russia. Russia signed the Palermo Convention on 12 December 2000 and ratified it on 26 April 2004 with reservations.[143] The Palermo Convention came into force on 25 June 2004. The reservations, which Russia made in relation to this convention mostly deal with mutual legal assistance and extradition and are described in Sections 6.3 and 6.4 below. Russia has implemented the provisions of the Palermo Convention. Further details on the implementation of these conventions are contained in sections 2.1 – 2.3.

740. Russia signed the TF Convention on 3 April 2000 and ratified it on 10 July 2002 with reservations[144]. The Convention came into force on 27 December 2002. Russia has implemented most of the provisions of this Convention, with reservations on mutual legal assistance and extradition similar to those made for the Palermo Convention. It should be noted that the TF offence does not extend to the theft of nuclear material [article 2(1)(a)]. See also section 2.2.

143 See Federal Law of 26.04.2004 no. 26-FZ.

144 See Presidential Instruction 24.03.2000 no 89-RP and Federal Law 10.07.2002 no 88-FZ.

741. Russia has not implemented the full range of measures relating to the freezing of TF funds under the United Nations Security Council Resolutions 1267 and 1373 and successor resolutions. The deficiencies noted in relation to the implementation of SR.III (its 1267 and 1373 component) are equally applicable in the context of SR.I (see section 2.4).

Additional elements

742. Russia also signed the Convention of the Council of Europe on laundering, search, seizure and confiscation of the proceeds from crime dated 8th November 1990 (with reservations). The Convention came into force in Russia on 1 December 2001. The 2005 Council of Europe Convention[145] on laundering, search, seizure and confiscation of the proceeds from crime has not been signed by Russia.

6.2.2 Recommendations and Comments

743. It is recommended that Russia correct the deficiencies noted in relation to the implementation of the relevant international conventions and UNSCRs as soon as possible. Russia should also institute criminal liability for legal persons.

744. Russia should implement the provisions of UNSCRs 1267, 1373 and successor resolutions (see section 2.4 of this report).

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**LC**	• TF Convention: article 2(1)(a) – theft of nuclear material is not covered.
SR.I	**LC**	• TF Convention: Article 2(1)(a) – theft of nuclear material is not covered. • UNSCRs 1267, 1373 and successor resolutions have been implemented insufficiently.

6.3 Mutual Legal Assistance (R.36-38, SR.V)

6.3.1 Description and Analysis

General

745. Russia is able to provide various forms of mutual legal assistance on the basis of provisions of the CCP[146] and of the AML/CFT Law[147]. Mutual Legal Assistance (MLA) is provided on the basis of international agreements or on a reciprocal basis. Reciprocity is established by an official letter of the requesting country expressing the willingness to provide MLA to Russia on a reciprocal basis. Mutual legal assistance requests are received by the General Prosecutor's Office (Directorate of International Legal Co-operation) and are disseminated to the law enforcement agencies, including the MIA, FSKN and the FSB. With countries where a reciprocal agreement based on a multilateral treaty does not exist, the MFA will nevertheless receive these requests and forward them to the General Prosecutor's Office. The Supreme Court receives MLA requests from the Supreme courts of other countries, and the MoJ receives MLA requests relating to all other levels of the court system.

746. At present, Russia has over 150 bilateral and multilateral agreements that were concluded at the state, governmental and interagency level and that relate to combating the crime and exchanging

145 The Convention entered into force on 1 May 2008.
146 Articles 457 – 459 of the CCP.
147 Article 10 AML/CFT Law.

information through MLA channels. Russia has concluded 34[148] bilateral agreements on mutual legal assistance in criminal matters. Moreover, Russia has entered into bilateral agreements on co-operation in the fight against crime with 44 countries[149], and with six countries[150] on co-operation and mutual assistance in combating illegal financial and AML operations. Russia is also party to more than 18 multilateral international anti-terrorist agreements.

747. Russia is a party to the following multi-lateral agreements which include provisions on mutual legal assistance:

- The European Convention on release 1957.
- European Convention on mutual legal assistance on criminal cases 1959.
- Two Conventions of the Commonwealth of Independent States – Conventions on Legal Assistance and Legal Relations on Civil, Family and Criminal Cases [Minsk (1993) and Kishinev (2002)].
- UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) (1988).
- UN Convention against Transnational Organised Crime (Palermo Convention) (2000).
- UN Convention against Corruption (2003).

748. Where there is no bilateral MLA treaty, Russia considers the Palermo Convention as a sufficient basis for MLA, including various investigative activities, freezing, seizing and confiscation, as well as extradition orders. This is specified in Palermo Convention and the UN Convention against Corruption Ratification Laws*[151]* and *[152].* According to the law, Russia uses the format of the Palermo convention relating to the procedures of MLA in instances where these norms provide for a higher degree of co-operation than an existing bilateral treaty (Law, 26-FZ, p.9-29 of article 18).

749. Some government bodies that engage in AML/CFT can execute requests from competent authorities of foreign states concerning confiscation of proceeds linked to ML/FT. Execution of such requests may involve: freezing property; performing examinations; questioning suspects, accused, witnesses and other persons; seizure of property; conducting searches; transferring material evidence; handling over and dispatching documents[153].

750. The MLA principles and procedures mentioned are equally applicable to combating terrorism financing.

---

148 Algeria, Angola, Azerbaijan, Albania, Bulgaria, Canada, China, Cuba, Cyprus, Czech Republic, Democratic People's Republic of Korea, Republic of Korea, Estonia, Hungary, India, Iraq, Iran, Greece, Kyrgyzstan, Latvia, Lithuania, Mexico, Mongolia, Moldova, Poland, Romania, Serbia (former Federal Republic of Yugoslavia), Spain, Slovakia, Tunisia, Turkey, United States, Vietnam and Yemen.

149 Austria, Argentina, Azerbaijan, Armenia, Albania, Belgium, Greece, Cyprus, Chile, China, Columbia, Cambodia, Egypt, Ecuador, Hungary, Israel, Italy, Ireland, Finland, France, Germany, Kyrgyzstan, Latvia, Laos, Moldova, Malta, Mexican, Norway, Panama, Portugal, Romania, Tajikistan, Turkmenistan, Slovenia, Sweden, Spain, South Africa, Turkey, United Kingdom, Ukraine, Uruguay, Uzbekistan, United Arabic Emirates and Vietnam.

150 Belarus, Bulgaria, Croatia, Georgia, Kazakhstan and Nigeria.

151 Federal Law no. 26-FZ (Palermo Convention), as well as Federal Law no.40-FZ (UN convention against corruption).

152 As the provisions of UN TOC and UN CAC are similar in relation to MLA, this report will reference Law no.26-FZ with a presumption to reference Law no.40-FZ as well.

153 Article 10 of Federal Law "On combating legalisation (laundering) of proceeds from crime and financing of terrorism"

Recommendation 36

751. The types of legal assistance which Russia can provide are listed in the CCP and in the AML/CFT Law (article 10). The requirements of the AML/CFT Law cover the requirements on the production, search and seizure of relevant documents and information, including financial information. Russia stated it has used these provisions in numerous cases relating to AML/CFT. Article 458 of the CCP provides for the transfer of relevant documents to the requesting country. The taking of evidence and statements from persons as well as the provision of evidentiary items is also covered, and this power has been exercised in practice by all of the relevant authorities – the FSKN, MIA, Prosecution Authority and the FSB. See Section 2.3 for the framework for the identification, freezing, seizure and confiscation of assets as well as assets of corresponding value and the instrumentalities of a crime. According to article 457 of the CCP representatives of the requesting country may be present during the execution of an MLA request by Russian authorities. Both the MIA and the Prosecution Authority informed that this is often the practice and serves as a means to ensure that an MLA request is satisfactorily fulfilled.

752. There are no disproportionate, unreasonable, or unduly restrictive conditions to the provision of MLA. The CCP serves as the procedural basis for executing MLA requests. The only condition placed on an MLA request is that it should not damage the sovereignty and security of Russia[154]. The evaluation team was informed that there were no refusals with reference to the ML/FT offences. At the same time article 457.2 of the CCP notes that the procedural legislative norms of a foreign country may be applied on a reciprocal basis or if relevant international treaties or bilateral agreements have been signed with this country.

753. The Prosecution Authority and executing authorities take into account any deadlines set out in the request. The CCP does not provide for a strict time limit to fulfil a request, however various regulations issued by the Ministries set a timeframe for executing a request. For example an order of the Minister of Internal Affairs, which handles most of the money-laundering related MLA requests, sets a 30-day timeframe[155]. Russia stated that the average time for fulfilling a request takes from one to two months and longer depending on the complexity of the request. Complaints concerning delays have been received from FATF and FSRB members. Some countries have complained that Russia needs up to 3 years to provide responses, without informing the requesting party of the reason for the delay. Russia stated that any delay to answer a request was usually due to the complexity of the case. In addition, Law No. 40-FZ notes that Russia will handle emergency MLA requests, if all of the procedures are observed. In order to facilitate the process of providing MLA, special MLA working groups are established with a number of countries. Currently at least four such working groups exist.

754. Russia indicated that fiscal issues, if part of an MLA request, will not serve as an impediment to a response. Financial secrecy laws do not seem to be an impediment to the provision of information through MLA mechanisms. The powers of law enforcement authorities to request from financial institutions information based on an open criminal case may be used in the circumstances of MLA. Examples have been provided on cases handled by the MIA and the FSB, which involved the transfer of such materials.

755. The powers of the relevant authorities under Recommendation 28 are available with regard to MLA requests. For a description of these measures see Section 2.6.

756. The procedures to avoid conflicts of jurisdiction in Russia are practical in nature. The Prosecution Authority makes a decision on the priorities for fulfilling a request when a number of foreign countries send requests on the extradition of the same person. The number of such cases is very limited, not more than 1 per year. The Prosecution Authority has to inform within 24 hours in writing the person who is to be extradited.

---

154 Article 457 of the CCP.

155 Order N 132 of 28.02.05.

Recommendation 37

757. Dual criminality is not a strict condition for the provision of MLA by Russia, except in relation to extradition. The evaluation team was informed that in the absence of mutual recognition of any relevant act as an offence (dual criminality) mutual legal assistance may be provided in the maximum possible degree. Technical differences between legislations of the requesting state and requested state are not an obstacle for Russia in provision of such assistance.

758. For those forms of mutual legal assistance where dual criminality is required, Russia appears to have no legal or practical impediment to rendering assistance where both countries criminalise the conduct underlying the offence.

Statistics

759. Russia provided the evaluation team with statistics related to *i)* the number of international requests for legal assistance in criminal cases related to money laundering, *ii)* the number of requests (related to money laundering) which have been answered, *iii)* the nature of requests (related to money laundering).

760. As the table below shows, the Russian authorities state that all requests have been answered in the year the request was received. This seems unlikely given the fact that feedback from FATF and FSRB members shows delays. The numbers also suggest that requests received at the end of the year are still answered before 31 December of that year. This is of course impossible, especially since, also according to Russia, all requests involved carrying out investigate actions. The evaluation team therefore considers these figures not to be reliable and therefore effectiveness could not be measured.

761. The Russian database does not provide statistics on the number of MLA requests refused. It was noted by the Russian authorities that there have been no cases of refusal in relation to ML/TF-related requests. All of these requests have been answered. Feedback on international co-operation with Russia showed that there have been cases of refusal, however this was not related to ML/FT. Most of the MLA requests on money-laundering are forwarded to the MIA. For example in 2005 the MIA handled 59 out of the 65 ML-related requests sent to Russia and in 2006 – 66 of the total 79 requests. For the most part the Department of Economic Security of the MIA is the unit handling the requests. The FSB, which also handles ML cases, as well as TF cases, received 24 such MLA requests in 2003 – 2006, however it was not clear what was the number of TF-related requests among those. One specific example of TF-related assistance was provided, which resulted in successful co-ordinated actions.

MLA requests related to ML		
MLA requests – received	**Year**	**Number**
	2003	3
	2004	4
	2005	65
	2006	79
	Total	**151**
MLA requests - answered	2003	3
	2004	4
	2005	65
	2006	79
	Total	**151**

Effectiveness

762. The Russian authorities provided numerous examples of how Russia handled various money laundering-related MLA requests, which resulted in successful investigations, prosecutions and convictions by foreign authorities as well as domestically within Russia. These examples covered the Prosecution Authority, MIA and FSB. This suggests some level of effectiveness. However, the full extent of the effectiveness of the international co-operation framework could not be completely ascertained, since reliable or accurate detailed, centralised statistics are not kept on all aspects of MLA requests made or received, relating to the predicate offences, ML or TF, or on the outcome of such requests. The feedback received from FATF and FSRB members points at some inefficiencies in the system, although, delays could also be attributed to the failings of requesting states.

Additional elements

763. In case of direct requests from foreign law enforcement bodies to Russian domestic law enforcement authorities the extent of co-operation will depend on bilateral and multilateral agreements between the parties. Such co-operation is also possible in accordance with the Palermo convention ratification Law, which according to this law should be used as a basis for law enforcement co-operation (article 1, p.8).

Recommendation 38

764. The relevant provisions on the identification, search, seizure and confiscation of criminal proceeds are contained in the CC, the CCP, relevant ratification laws and the AML/CFT Law. The general legal framework of Russia described above in relation to Recommendation 36 applies to identification, search, seizure and confiscation issues. For a more detailed review of the domestic confiscation mechanisms, see section 2.4.

765. According to article 10 of the AML/CFT Law the transfer of information connected with the tracing, seizure and confiscation of proceeds from crime to the competent bodies of a foreign state can be carried out, if it does not damage the interests of national security of Russia, and allows the competent bodies of this foreign state to commence investigation or an inquiry. This information can be transferred provided that it will not be used for purposes not mentioned in the information request. According to the same article the competent authorities are required to handle tracing, seizure and confiscation requests of foreign authorities.

766. Article 104.2 CC provides for the possibility of confiscation of property of corresponding value. If the confiscation of a certain object is impossible due to its use, sale or for any other reason the court will issue the judgment on confiscation of the amount of money which corresponds to the cost of such object.

767. According to article 11 of the AML/CFT Law and on the basis of a specific international agreement criminal proceeds or property of corresponding value may be transferred completely or partially to the foreign state whose court made the decision on confiscation. No requests for confiscation of property were received by the Prosecution Authority.

768. Russia has a number of bilateral and multilateral arrangements with foreign counterparts regarding matters of seizure and confiscation[156] and is able to share assets with foreign countries. The Kishinev Convention among CIS states contains a framework for search, seizure and confiscation

[156] The bilateral treaties are with Angola, Canada, India, Korea, Mexico and the United States. The multilateral treaties are the UN Convention against transnational organized crime of 15.11.2000; UN International Convention for the Suppression of the Financing of Terrorism of 09.12.1999; Convention of the CoE on laundering, search, seizure and confiscation of the proceeds from crime of 08.11.1990; UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances of 20.12.1988; The Single Convention on Narcotic Drugs of 30.03. 1961; European Convention on Extradition of 13.12.1957.

among the signatories (article 104). Russia has not shared assets recently with foreign counties (and vice versa).

769. Russia considered the creation of an asset forfeiture fund in 2002 when the AML/CFT system was being set up. The mechanism, which currently exists, provides for the transfer of confiscated property to the Russian Federal Property Fund (established by Government Decree No. 925 dated December 12, 2002). The property is then auctioned and the proceeds from the auction are transferred to the federal budget, which is spent on various programmes, largely of a social nature.

770. Russia can recognise and enforce foreign non-criminal confiscation orders. No statistics were provided.

Effectiveness

771. The necessary mechanisms are in place for international co-operation on confiscation measures, however they have not yet been tested in practice because Russia has not received any foreign confiscation requests to date.

6.3.2 Recommendations and Comments

772. It is recommended that the Russian authorities continue to institute a pro-active approach to monitoring progress on execution of requests and better ensuring a timely and effective response.

773. The General Prosecutor's Office should ensure that clear lines of communication exist with established points of contact between itself and the law enforcement officer responsible for execution of the request, as well as between itself and the requesting country.

774. It is recommended that the authorities maintain statistics on the more detailed aspects of MLA including details on the nature and results of MLA requests.

775. The Russian authorities are encouraged to continue their monitoring of the process of providing MLA among special MLA working groups established with a number of countries.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3 underlying overall rating
R.36	**LC**	• No reliable statistics provided to show effectiveness of the system. • Feedback from other FATF and FATF-style Regional Bodies shows delay in answering MLA requests.
R.37	**C**	• This Recommendation is fully observed.
R.38	**C**	• This Recommendation is fully observed.
SR.V	**LC**	• The deficiencies related to Recommendations 36 and 39 have a negative effect on the rating of this Recommendation.

6.4. Extradition (R.37, 39, SR.V)

6.4.1 Description and Analysis

776. Extradition procedures in Russia are based on a range of key international instruments dealing with extradition, which include among others the relevant universal conventions (Vienna (1988) and Palermo (2000) Conventions, UN Convention against corruption (2003), European treaties (European Convention on Extradition (1957) and its Additional Protocols (1975, 1978), as well as the CIS Minsk (1993) and Kishinev (2002) Conventions), that Russia is a party to.

777. In relation to AML investigations, Russia has extradited individuals through bi-lateral treaties to four countries[157]. Russia has bilateral treaties with another 30 countries[158]. Russia is also a party to two multilateral treaties[159].

778. Money laundering is an extraditable offence in Russia. The main provisions of the national legislation relating to extradition are contained in the Constitution (articles 61, 63), in Chapters 54-55 of the Code of Criminal Procedure as well as in the AML/CFT Law. As money laundering is a criminal offence in Russia, it is extraditable if the conduct for which extradition is sought is criminalised and punishable by a custodial sentence of at least one year in both the requested and requesting states (according to article 462 of the CCP). According to article 12 of the AML/CFT Law, Russian authorities are required to handle extradition requests regarding MLA in the framework of international agreements of Russia. According to article 1.3 of Federal Law No. 26 Russia considers the Palermo Convention as a legal mechanism for extradition. Similar provisions are contained in article 1.2 of the Law No. 40-FZ, which ratified the UN Convention against Corruption.

779. In the execution of a request for extradition, the standards of the CCP generally apply, however, according to article 457 the procedural standards of the foreign state can apply, in accordance with international agreements of Russia, on a mutual basis, unless this contradicts the laws and international liabilities of Russia.

780. According to article 61 of the Constitution and article 464 of the Code of Criminal Procedure, Russian citizens cannot be extradited to the territory of a foreign state. However, according to article 12 CC, citizens of Russia and stateless persons with a permanent residence in Russia, who have committed offences beyond the territory of Russia, are criminally liable if the act is considered an offence in the state where it has been committed, if these persons were not convicted in the foreign state, the criminal case can be opened[160], investigated using the materials provided by the foreign competent authority, and prosecuted by the Prosecution Authority in accordance with the CCP. In such situations, the materials provided by foreign authorities may be used to the fullest extent possible according to procedures of the CCP relating to MLA.

781. According to article 462 of the CCP, to article 12 of Federal Law No. 115-FZ, as well as on the basis of international treaties and principle of reciprocity, Russia can extradite a foreign citizen or stateless person, staying in the territory of Russia to a foreign state for criminal prosecution or to serve a sentence for money laundering or terrorist financing or for the predicate offences. Such persons may be extradited if the mentioned offences are punishable under the criminal law and laws of the foreign state that submitted the extradition request.

782. Dual criminality is required under the CCP for extradition. In this regard the deficiencies noted in the criminalisation of ML (insider trading and stock market manipulation not criminalised) and TF (theft of nuclear material not covered) may prove to be an obstacle in executing extradition requests.

---

157 Angola, Brazil, China and India.

158 Azerbaijan, Algeria, Bosnia and Herzegovina, Bulgaria, Croatia, Cuba, Cyprus, Czech Republic, Estonia, Finland, Greece, Hungary, Iran, Iraq, the DPRK, Kyrgyzstan, Latvia, Lithuania, Macedonia, Moldova, Mongolia, Montenegro, Poland, Rumania, Serbia, Slovakia, Slovenia, Tunisia, Vietnam and Yemen.

159 The European Convention on Extradition of December 13, 1957 (Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Liechtenstein, Lithuania, Luxemburg, Macedonia, Malta, Moldova, Montenegro, the Netherlands, Norway, Poland, Portugal, Rumania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and Ukraine), and the Convention on legal assistance and legal relations in civil, family and criminal matters of January 22, 1993 (Azerbaijan, Armenia, Belarus, Georgia, Kyrgyzstan Uzbekistan, Kazakhstan, Moldova, Tajikistan, Turkmenistan, Ukraine.

160 For example immunity against criminal prosecution would prevent a case from being opened.

783. Information provided by Russian authorities indicated that technical differences in criminalising the conduct are not an obstacle in this case to executing an extradition request, as is the practice in relation to other forms of MLA.

784. Extradition is not admissible if the person, with respect to whom the request for extradition has come from a foreign state, has been granted asylum in Russia because of the possibility of his persecution in that state on account of race, religion, citizenship, nationality, affiliation with a certain social group, or because of his political views (item 2 of article 464 of the CCP). Rejection of the request for extradition of persons accused of financing terrorism on the basis of political grounds is not admissible, as provided for by the Federal Law ratifying the TF Convention.

785. Where the subject of an extradition request made to Russia is also the subject of domestic proceedings against him or her, then the domestic proceedings will take precedence, with an obvious impact on the timeframe in which extradition cases can be handled. Otherwise, the CCP instructs the Prosecution Authority to execute requests without unnecessary delay (CCP, articles 460 – 467).

786. The specific procedures for extradition are established by the Prosecution Authority in the Extradition Instruction[161]. The instruction describes detailed procedures to be followed by the territorial and federal prosecutors in relation to extradition and includes the specific time frames for the execution of all of the procedural actions. The instruction describes the detailed components of the actions themselves, including the appeal process. For serious crimes the instruction demands a simplified and expedited procedure of extradition. It also creates a mechanism, where prosecutors of all levels regularly report on the implementation of this instruction.

787. The extradition provisions of Russian legislation in relation to money laundering are equally applicable in cases of terrorism financing.

Additional elements

788. Simplified procedures of extradition by way of permission for direct transfer of requests for extradition between relevant designated competent authorities exist. At the same time a simplified procedure of consenting persons is not stipulated. Persons cannot be extradited only on the basis of a warrant for arrest or court decision.

Statistics

789. Russia provided the evaluation team with statistics related to *i)* extradited persons from Russia to foreign states under article 262 of the CCP, *ii)* received requests for criminal prosecution of Russian citizens having committed crimes on territory of foreign state, and *iii)* executed requests for criminal prosecution of Russian citizens having committed crimes on the territory of foreign state. All these statistics can be found in the tables below. There is no breakdown available for ML and / or TF related requests, but it was known that at least four persons were extradited for ML to Ukraine.

Extradition requests to and from Russia (all crimes)			
	Year (2007 up to October only)	**Number**	
		CIS countries	**Other countries**
Number of persons extradited from Russia (CCP, article 262)	2006	1048	16
	2007	810	16
		All countries	

[161] Instruction of the General Prosecutor's Office no. 32/35 of 20.06. 2002 "On the procedure of the consideration of foreign states' requests on extradition in view of the entrance into force of the CCP".

Extradition requests to and from Russia (all crimes)		
Requests to Russia for prosecution of Russian citizens in Russia for crimes committed abroad.	2006	215
	2007	123
Executed requests to Russia for prosecution of Russian citizens in Russia for crimes committed abroad.	2006	159
	2007	121

790. The data provided demonstrates that the extradition system is functioning rather effectively; however, more detailed information on the various aspects of the extradition process were not provided. In the absence of complete statistics it is not possible to make an assessment of effectiveness. The data, however, do show that extradition heavily focuses on CIS countries. While this is to be expected, due to geographic proximity and high degrees of similarity of legal systems, the current numbers are still too low for non-CIS countries.

6.4.2 Recommendations and Comments

791. Russia should further enhance the existing system of reviews in relation to extradition according to Instruction No. 32/35 and maintain comprehensive statistics in relation to ML/TF covering all details of the extradition process.

792. Russia should also raise the effectiveness of its extradition practice in relation to non-CIS countries and make the figures for CIS and non-CIS countries better comparable. Russia is however to be commended for the high number of requests to and from CIS countries.

793. Russia should address the missing elements of its ML and TF offences to ensure that dual criminality requirements do not represent an obstacle for extradition in such matters (see also sections 2.1 and 2.2 for discussion of the missing elements of the ML and TF offences).

6.4.3 Compliance with Recommendations 37 & 39, and Special Recommendation V

	Rating	Summary of factors relevant to s.6.4 underlying overall rating
R.39	**LC**	• Deficiencies noted in relation to the criminalisation of ML and TF may prove to be an obstacle in executing extradition requests. • The effectiveness of the extradition system to and from non-CIS countries should be enhanced.
R.37	**C**	• This Recommendation is fully observed.
SR.V	**LC**	• The deficiencies related to Recommendations 36 and 39 have a negative effect on the rating of this Recommendation.

6.5 Other Forms of International Co-operation (R.40 & SR.V)

6.5.1 Description and Analysis

794. The general provision on (international) information exchange is set out in article 10 of the AML/CFT Law. The provision is quite broad and concerns all authorities that are concerned in the fight against ML/FT. This provision for the most part covers the elements of Recommendation 40. Even though all agencies concerned can act internationally on their own initiative, most of the international co-operation takes place through Rosfinmonitoring. On the policy level, Rosfinmonitoring is the authority that represents Russia in FATF, EAG, MONEYVAL and the Egmont Group.

795. Rosfinmonitoring exchanges information through the Egmont Group and has, in addition, 39 MOUs with other FIUs[162]. It is currently discussing MOUs with ten other countries.

796. As of December 2007, the BoR had concluded 21 agreements (MOUs) which included statements on co-operation in the area of AML/CFT[163]. In addition, the BoR reported that it was considering agreements with another five countries. Article 51 of the BoR Law gives the BoR the right to request information from foreign supervisory authorities, and to provide information that does not contain information on the operations of credit institutions or their customers.

797. The Russian authorities report that the time period for execution of international requests for assistance is usually set out in the relevant MOU, but there is a default time limit of one month from the date of receipt of the request (BoR Guidance N 1381-U – not provided to the evaluation team).

798. The Russian authorities were not able to provide information about refused requests for assistance.

799. The BoR reports that it received and answered 18 requests for international assistance between 2003 and 2006. However, no further details of from who these requests were received or their nature were made available to the evaluation team.

800. The BoR is able to request and provide information to the corresponding banking supervisor received in the execution of its supervisory function. No further information was made available to the evaluation team.

801. The FISS has an MOU with the USA, and is an active member of the IAIS.

802. The Federal Financial Markets Service is a member of the International Organisation of Securities Commissions.

6.5.2 Compliance with Recommendation 40 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40	**C**	• This Recommendation is fully observed.

7. OTHER ISSUES

7.1 Resources and statistics

803. The text of the description, analysis and recommendations for improvement that relate to Recommendations 30 and 32 is contained in all the relevant sections of the report (*i.e.* all of section 2, parts of sections 3 and 4, and in section 6). There is a single rating for each of these Recommendations, even though the Recommendations are addressed in several sections. Section 7.1 of the report only contains the box showing the rating and the factors underlying the rating, and includes a cross-reference to the relevant section and paragraph in the report where this is described.

[162] Afghanistan, Armenia, Belarus, Belgium, Brazil, Bulgaria, China, Columbia, the Czech Republic, Cyprus, Egypt, Estonia, Finland, France, Germany, Israel, Italy, Korea, Kyrgyzstan, Latvia, Liechtenstein, Luxemburg, Macedonia, Mexico, Moldova, Monaco, Montenegro, Panama, Peru, Poland, Portugal, Rumania, Slovenia, South Africa, Sweden, the United Kingdom, Ukraine, the United States and Venezuela.

[163] Armenia, Azerbaijan, Belarus, China, Cyprus, Finland, Georgia, Germany, Kyrgyzstan, Latvia, Lithuania, Macedonia, Moldova, Mongolia, Montenegro, Panama, Norway, Tajikistan, Turkmenistan, Venezuela and Vietnam.

804. With the exception of the staff of one regional law enforcement body that indicated that its resources were insufficient and with the exception of Rosfinmonitoring headquarters in Moscow that indicated that its resources were sufficient, most other interviewed agencies appeared to be uncomfortable in discussing areas in which additional resources (such as staff or budget) would be needed. The staff of Rosfinmonitoring headquarters equally was uncomfortable in indicating which other agencies, in their view, have sufficient or insufficient resources. Nonetheless, Rosfinmonitoring headquarters did provide the evaluation team with sufficient statistics to assess the resources of some agencies. Overall, however, because of these reasons and because the statistics are confidential (see section 2.6 of this report), the evaluation team could not fully assess the effective implementation of this Recommendation for all agencies involved in the fight against money laundering. This has a negative effect on the rating.

	Rating	Summary of factors relevant to Recommendations 30 and 32 and underlying overall rating
R.30	**PC**	• For a majority of regional offices and for a majority of law enforcement and supervisory agencies, the number of staff specifically devoted to AML/CFT issues is low, or was difficult to assess.
R.32	**LC**	• Not all authorities keep quality statistics on matters relevant to the effectiveness and efficiency of the system.

TABLES

TABLE 1: RATINGS OF COMPLIANCE WITH FATF RECOMMENDATIONS

The rating of compliance vis-à-vis the FATF Recommendations should be made according to the four levels of compliance mentioned in the 2004 Methodology (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC), or could, in exceptional cases, be marked as not applicable (N/A).

Forty Recommendations	Rating	Summary of factors underlying rating
Legal systems		
R.1 ML offence	LC	• Russia has not established offences of insider trading and stock market manipulation.
R.2 ML offence – mental element and corporate liability	LC	• Russia has not established criminal liability for legal persons.
R.3 Confiscation and provisional measures	C	• This Recommendation is fully observed.
Preventive measures		
R.4 Secrecy laws consistent with the Recommendations	C	• This Recommendation is fully observed
R.5 Customer due diligence	PC	• No specific prohibition on maintaining existing accounts in fictitious names. • No requirement to conduct CDD if suspicion of ML/TF if one of the exemptions of AML/CFT Law article 7 clause 1.1 applies. • No requirement in Law or Regulation for dealing with doubts about veracity. • Lack of clarity and effectiveness in respect of beneficial ownership requirements. • Lack of clarity in relation to ongoing due diligence. • No direct requirement to establish nature and intended purpose of business relationship. • Doubts about clarity and effectiveness of requirements relating to SDD and EDD. • Timing of verification – no measures for non-CIs. • Failure to complete CDD – measures for non-CIs only extend to ID.
R.6 Politically exposed persons	PC	• Definition of PEPs does not extend to those who *have been* entrusted with public functions. • No requirement for obtaining approval from senior management for existing customers found to be PEPs. • Lack of clarity relating to establishing source of wealth and enhanced ongoing due diligence. • Beneficial ownership is not covered. • No information on effectiveness.
R.7 Correspondent banking	PC	• No specific requirement to understand nature of respondent's business or determine quality of supervision.

Forty Recommendations	Rating	Summary of factors underlying rating
		• No requirement to ascertain if respondent has been subject of ML/TF investigation. • Nothing specific requiring a judgement on effectiveness of respondent AML/CFT system.
R.8 New technologies & non face-to-face business	PC	• Requirements for new technologies limited to internet banking. • No requirements for non face-to-face transactions except for CIs.
R.9 Third parties and introducers	N/A	• This recommendation is not applicable (financial institutions are legally not permitted to rely on intermediaries or third parties).
R.10 Record keeping	LC	• Account files and business correspondence do not have to be kept for a minimum of five years from the termination of the account or the business relationship. • "Timely access" is not required by law or regulation.
R.11 Unusual transactions	PC	• No requirement for FIs to examine as far as possible the background and purpose of all unusual transactions. • No requirement for FIs to set forth the findings of such examinations in writing. • No specific requirement for FIs to keep such findings available for competent authorities and auditors for at least five years. • Lack of effectiveness, especially in the non CI sector.
R.12 DNFBP – R.5, 6, 8-11	PC	*Applying R.5* • Casinos/Real Estate Agents/Dealers in Precious metals and stones – similar technical omissions as recorded under R 5. In particular: o No requirement for dealing with doubts about veracity of previously obtained information. o Lack of clarity and effectiveness in respect of beneficial ownership requirements. o Lack of clarity in relation to ongoing due diligence. o Doubts about clarity and effectiveness of requirements relating to SDD and EDD. o Timing of verification – no requirements. o Failure to complete CDD requirements limited to failure to carry out customer ID. o Concerns about effectiveness in the casino sector. • Lawyers/notaries/accountants o CDD requirements only relate to ID. *Applying R.6* • Lawyers/notaries/accountants: New provisions do not apply. • All other entities: similar omissions as recorded under R 6. *Applying R.8* • Casinos: requirements limited to prohibition of gambling via the internet. • All other entities: no requirements except the need to personally identify all natural persons. *Applying R.9* • N/A *Applying R.10* • Casinos/Real Estate Agents/Dealers in Precious metals and stones o Similar omissions as recorded under R 10. • Lawyers/notaries/accountants • No requirement to keep records except for those relating to ID.

Forty Recommendations	Rating	Summary of factors underlying rating
		Applying R.11 • All designated assessed sectors ○ Similar omissions as recorded under R 11, practice suggests concentration on factors which give rise to the submission of STRs. • All Recommendations: TCSPs are not covered. • Accountants – no information on effectiveness.
R.13 Suspicious transaction reporting	LC	• No STR requirement in cases possibly involving insider trading and market manipulation. • No general STR requirement for attempted transactions by occasional customers. • Shortcoming in the criminalisation for terrorist financing limits the reporting obligation. • Lack of effectiveness, specifically relating to the TF STR system.
R.14 Protection & no tipping-off	PC	• FIs themselves and their directors are not covered by the safe harbour provision and the tipping off prohibition.
R.15 Internal controls, compliance & audit	PC	• Internal control procedures governing terrorism financing lack a comprehensive treatment of CFT, focusing almost exclusively on a "list-based" approach. • Training programmes of FIs focus too heavily on legal requirements under the AML/CFT Law, rather than on practical case studies of ML and TF, diminishing the effectiveness of the programmes. • Screening programmes are not broad enough, do not cover all personnel and do not focus on country specific risks, diminishing the effectiveness of the programmes. • Russia Post could not demonstrate effective implementation of internal control programmes at all branches.
R.16 DNFBP – R.13-15 & 21	PC	*Applying R.13* • Similar technical concerns to those recorded under Recommendation 13. • Casinos: Inconsistent levels of reporting lead to some doubts about effectiveness. • Real estate agents: Historically, relatively few STRs submitted. • Dealers in precious metals and stones: Large sector with relatively few STRs; lack of clarity as to how many STRs relate to the sector covered by the FATF definition. • Lawyers/notaries: Few STRs in this sector give rise to concerns over effectiveness. • Accountants – No specific information received. *Applying R.14* • Similar technical concerns to those recorded under Recommendation 14. *Applying R.15* • Casinos/real estate agents/dealers in precious metals and stones – similar technical concerns to those recorded under Recommendation 15, and overall doubts about effectiveness. • Lawyers/notaries/accountants – Doubts about effectiveness given the lack of AML/CFT supervision of lawyers and accountants and lack of information about supervision of notaries. *Applying R.21* • No relevant requirements.

Forty Recommendations	Rating	Summary of factors underlying rating
		• All Recommendations: TCSPs are not covered. • Accountants – no information on effectiveness.
R.17 Sanctions	PC	• Maximum fines that can be imposed by the BoR are too low. • Article 15.27 Code of Administrative Offences is not sufficiently broad. • Maximum fines against officials of financial institutions are too low. • No powers for supervisors (other than the BoR) to replace directors / senior management. • No powers for the BoR, the FSFM, the FISS and ROSCOM to withdraw a licence when the owners are convicted of a relevant criminal or economic offence. • System to sanction financial institutions other than credit institutions is not effective.
R.18 Shell banks	C	• This Recommendation is fully observed.
R.19 Other forms of reporting	C	• This Recommendation is fully observed.
R.20 Other NFBP & secure transaction techniques	C	• This Recommendation is fully observed.
R.21 Special attention for higher risk countries	PC	• No requirement for financial institutions to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. • No requirement to examine as far as possible the background and purpose of such business relationships and transactions, to set forth the findings of such examinations in writing and to keep such findings available for competent authorities and auditors for at least five years.
R.22 Foreign branches & subsidiaries	NC	• The legal and regulatory framework does not consistently apply the requirement to abide by Russian AML/CFT Laws and regulations to both foreign branches and subsidiaries. • Existing guidance on foreign operations of CIs applies only to prudential risks, not to AML/CFT requirements. • There is no requirement for increased vigilance over foreign operations in jurisdictions that do not or insufficiently apply FATF recommendations. • There is no specific requirement to inform the Russian regulator when a foreign branch, subsidiary or representative office is unable to observe appropriate AML/CFT measures. • Foreign operations of non-credit FIs are not covered by the existing regulatory regime, thus effectiveness of the current legal framework cannot be assessed.

Forty Recommendations	Rating	Summary of factors underlying rating
R.23 Regulation, supervision and monitoring	PC	• No provisions to prevent criminals from becoming major shareholders in a non-banking financial institution. • Inadequate threshold with respect to major shareholders of credit institutions. • Inadequate provision regarding persons having a controlling interest with respect to a credit institution. • No fit and proper requirement regarding leasing companies and the members of the board of a life insurance company or an insurance broker. • No fit and proper test and general lack of effectiveness regarding the system to register and supervise organisations providing MVT services according to article 13.1 Banking Law. • Lack of effectiveness with respect to the supervision of the FSFM, the FISS and ROSCOM.
R.24 DNFBP - regulation, supervision and monitoring	PC	• No current AML/CFT licensing regime by an AML/CFT competent authority for casinos. • No measures to prevent criminals holding an interest in a casino. • Limited number of focused supervisory visits to real estate agents. • As reported on-site, supervisory activity for casinos does not appear to be proportionate to the perceived risks identified by the supervisor. • Monitoring of lawyers is remote and not specific to AML/CFT. • No details of specific AML/CFT monitoring of notaries. • Assay Chamber does not consider itself to have adequate powers. • Assay Chamber has relatively few AML/CFT specialists to supervise 25 000 firms. • General lack of specific information to assess effectiveness of the sanctions regime relating to DNFBPs. • TCSPs not covered.
R.25 Guidelines & Feedback	PC	• Insufficient and ineffective guidance to FIs, beyond an explanation of the law. • No case-by-case feedback beyond the acknowledgement of the receipt of the STR. • Limited feedback given to the dealers in precious metals and stones, lawyers and notaries. • No information about feedback given to accountants.
Institutional and other measures		
R.26 The FIU	C	• This Recommendation is fully observed.
R.27 Law enforcement authorities	LC	• The discretionary powers of the Prosecution Authority to transfer a case from one law enforcement to another may lead to a lack of clear distribution of money laundering cases among law enforcement bodies (effectiveness issue). • Corruption has an impact on the effectiveness of the system. • Some designated law enforcement bodies do not appear to have sufficient knowledge of the ML provisions.
R.28 Powers of competent authorities	C	• This Recommendation is fully observed.

Forty Recommendations	Rating	Summary of factors underlying rating
R.29 Supervisors	PC	• Limitation on the BoR for conducting on-site AML/CFT inspections. • FISS not able to compel and obtain access to information protected by banking secrecy. • Maximum fines against credit institutions are too low. • No power for the BoR to fine directors or senior management. • No powers for the FSFM, the FISS and ROSCOM to impose fines on financial institutions and directors / senior management and to replace directors / senior management. • No powers for the BoR, the FSFM, the FISS, ROSCOM and Rosfinmonitoring to withdraw a licence when the owners are convicted of a relevant criminal or economic offence. • System to sanction financial institutions other than credit institutions is not effective. • Lack of clarity with respect to ROSCOM's competence to carry out on-site inspections related to the full set of AML/CFT requirements and to compel production of records.
R.30 Resources, integrity and training	PC	• For a majority of regional offices and for a majority of law enforcement and supervisory agencies, the number of staff specifically devoted to AML/CFT issues is low, or was difficult to assess.
R.31 National co-operation	LC	• Law enforcement agencies and supervisors do not adequately co-operate on the operational-level with respect to potential systemic vulnerabilities such as illegal money and value transfer services.
R.32 Statistics	LC	• Not all authorities keep quality statistics on matters relevant to the effectiveness and efficiency of the system.
R.33 Legal persons – beneficial owners	PC	• None of the existing systems achieve adequate transparency regarding the beneficial ownership and control of legal persons.
R.34 Legal arrangements – beneficial owners	N/A	• This recommendation is not applicable.
International Co-operation		
R.35 Conventions	LC	• TF Convention: article 2(1)(a) – theft of nuclear material is not covered.
R.36 Mutual legal assistance (MLA)	LC	• No reliable statistics provided to show effectiveness of the system. • Feedback from other FATF and FATF-style Regional Bodies shows delay in answering MLA requests.
R.37 Dual criminality	C	• This Recommendation is fully observed.
R.38 MLA on confiscation and freezing	C	• This Recommendation is fully observed.
R.39 Extradition	LC	• Deficiencies noted in relation to the criminalisation of ML and TF may prove to be an obstacle in executing extradition requests. • The effectiveness of the extradition system to and from non-CIS countries should be enhanced.
R.40 Other forms of co-operation	C	• This Recommendation is fully observed.
Nine Special Recommendations		
SR.I Implement UN instruments	LC	• TF Convention: Article 2(1)(a) – theft of nuclear material is not covered. • UNSCRs 1267, 1373 and successor resolutions have been

Forty Recommendations	Rating	Summary of factors underlying rating
		implemented insufficiently.
SR.II Criminalise terrorist financing	LC	• The terrorist financing offence does not extend to the theft of nuclear material, as required in the UN Convention for the Suppression of the Financing of Terrorism. • Russia has not established criminal liability for legal persons.
SR.III Freeze and confiscate terrorist assets	PC	• Reliance on the criminal justice system risks creating problems with the effective implementation of UNSCR 1373. • Russia does not have a national mechanism to examine and give effect to freezing actions taken by other countries. • Russia does not have an effective and publicly-known mechanism for the purpose of considering de-listing requests. • Russia does not have an effective and publicly-known procedure for unfreezing the funds of persons inadvertently affected by a freezing action.
SR.IV Suspicious transaction reporting	PC	• No STR requirement for attempted transactions by occasional customers. • Shortcoming in the criminalisation for terrorist financing limits the reporting obligation. • Lack of effectiveness, specifically relating to the TF STR system.
SR.V International co-operation	LC	• The deficiencies related to Recommendations 36 and 39 have a negative effect on the rating of this Recommendation.
SR VI AML requirements for money/value transfer services	NC	• The current system lacks effectiveness in ensuring compliance. • Insufficient attention is devoted to the existence of and risks presented by illegal alternative remittance systems. • Payment acceptance service providers were not covered by supervisory regime until November 2007, therefore effectiveness of their compliance with AML/CFT rules cannot be determined. • Implementation of Recommendations 5, 6, 7, 8, 10, 13, 14, 15, 22 and 23 in the MVT sector suffers from the same deficiencies as those that apply to banks. • ROSCOM lacks effective sanctioning powers.
SR VII Wire transfer rules	PC	• Full originator information is not required in certain limited cases. • No requirements for beneficiary FIs to adopt a risk-based procedure for wire transfers, and incoming transfers are not covered at all. • Requirement to refuse transactions without full originator information cannot be implemented. • Batch transfers are not specifically mentioned in the Law. • Shortcomings identified under Recommendation 17 (sanctions) and 23 (monitoring and supervision) apply equally to this Special Recommendation. • Effectiveness of the new system cannot be measured.
SR.VIII Non-profit organisations	PC	• The lack of a comprehensive review of the system means that not all the necessary measures have been taken and it is unclear what measures are part of a comprehensive policy to fight the misuse of NPOs by terrorist financiers, and what the effect of those measures has been (effectiveness issue). • Some of the rules are insufficiently enforced. • There is inconsistent outreach to the NPO sector to provide guidance. • There is no formalised and efficient system in place that focuses on potential vulnerabilities. • There is no formalised and efficient system in place to share

Forty Recommendations	Rating	Summary of factors underlying rating
		information to target abuse. • No single authority is formally designated as the competent authority responsible for co-ordinating Russia's domestic efforts regarding NPOs and receiving international requests.
SR.IX Cross Border Declaration & Disclosure	NC	• No clear power to stop or restrain declared cash or bearer negotiable instruments in case of a suspicion of money laundering. • Customs declaration forms are not in line with the requirements set in the law. • Customs authorities do not keep all required data relating to ML/TF. • There is inadequate co-ordination among relevant competent authorities on cross border cash movement (effectiveness). • The administrative fines available for false or non-declarations are not dissuasive and not effective. • Customs staff seem not to be aware that the system can be used for AML/CFT purposes (effectiveness). • Insufficient number of dedicated AML/CFT staff at the borders. • Corruption seems to affect the effectiveness of the system. • Failures under Special Recommendation III have a negative impact. • Sending cash through containerised cargo is not covered and implementation through general provisions was not demonstrated. • The authorities could not demonstrate the effectiveness of the system.

TABLE 2: RECOMMENDED ACTION PLAN TO IMPROVE THE AML/CFT SYSTEM

Recommended Action	
Section 2. Legal System and Related Institutional Measures	
2.1 Criminalisation of ML (R.1 & 2)	• Russia should establish offences of insider trading and stock market manipulation. • Russian authorities should reconsider their position concerning the criminal liability of legal persons.
2.2 Criminalisation of TF (SR.I)	• Russia should establish the offence of theft of nuclear material and expand the TF offence to include this new offence. • Russian authorities should reconsider their position concerning the criminal liability of legal persons.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• Russia should consider expanding the confiscation provisions in its Criminal Code article 104.1 to include at the very least the money laundering offence.
2.4 Freezing of funds used for terrorist financing (SR.III)	• Russia should implement the elements of SR.III that go beyond the requirements of the UNSCRs. • Russia should rely less on the criminal justice system to be able to effectively implement SR.III. • Russia needs to implement a national mechanism to examine and give effect to actions initiated under the freezing mechanisms of other jurisdictions. • Russia should establish an effective and publicly known procedure for dealing with de-listing requests and for dealing with requests to unfreeze in a timely manner the funds or other assets of entities that have been inadvertently affected by a freezing action.
2.5 The Financial Intelligence Unit and its functions (R.26)	• The number of personnel vacancies at Rosfinmonitoring is somewhat high and all vacancies should be filled as a priority matter.
2.6 Law enforcement, prosecution and other competent authorities (R.27 & 28)	• The initiation of a general discussion on how to define and determine the competences of law enforcement agencies and their specialised units in ML/TF cases would be beneficial. • The Prosecution Authority should implement more rigorous supervision to at least to be able to be aware of all cases pursued by law enforcement bodies. • Efforts to eliminate corruption should continue and deepen. • All law enforcement authorities should continue to strengthen the existing inter agency AML/CFT training programmes in order to have specialised financial investigators and experts at their disposal. • International training programmes on ML and FT issues, especially for law enforcement staff in the (border) regions, should be enhanced. • The low number of ML convictions in comparison with the number of detected ML crimes should be addressed and consideration should be given to a greater specialisation within the Prosecution Authority and the judiciary, including establishing specialised units within Prosecution Authority and specialised courts for ML and FT, in order to increase the effectiveness of the system.
2.7 Cross Border Declaration & Disclosure	• Russia should implement all elements of an effective system to deter illegal cross border movements of currency. • Staffing levels of the FCS should be increased to keep up with the growing workload. • The FCS should be encouraged to continue fighting corruption. • Authorities should as a priority commence an awareness raising campaign, for all levels of staff in all regions. • The authorities should ensure that customs and law enforcement co-operate in all regions and are aware of each others' cases, especially relating to the fight against alternative remittance systems. • The legal framework for reporting cash and bearer negotiable instruments should be simplified in one law, and reporting forms should be brought in line with the law in all languages.

Recommended Action	
	• Russia should ensure that sending cash or bearer negotiable instruments through containerised cargo is covered in law and practice. • The FCS should have the legal authority to restrain currency in case of suspicions of ML if the money is declared. The FCS should take into consideration a system to use reports on currency declaration in order to identify and target money launderers and terrorists. • The administrative penalties for false or non declarations should be raised considerably.
Section 3. Preventive Measures – Financial Institutions	
3.1 Risk of money laundering or terrorist financing	• No recommendations.
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	*Recommendation 5* • Russia should ensure that the following issues are covered by law or regulation: (i) a specific prohibition on maintaining existing accounts under fictitious names, (ii) a requirement to carry out CDD where there is a suspicion of money laundering, regardless of any exemptions, (iii) performance of CDD where there are doubts about the veracity of previously obtained customer identification data, (iv) a requirement to identify beneficial owners and in particular to establish the ultimate natural owner/controller and (v) requirements for conducting ongoing due diligence. • The following matters should be set out in law, regulation or other enforceable means: (i) requirement for non-CIs to understand the ownership or control structure of a legal person, (ii) requirement to ascertain the purpose and intended nature of the business relationship, (iii) requirements for the timing of verification of identification, and (iv) consequences of a failure to conduct CDD. • Requirements relating to enhanced and simplified due diligence should be clarified, in particular the exemptions from conducting CDD in situations relating to occasional transactions. Further guidance to FIs on dealing with legal arrangements from overseas would be helpful. • A stronger link in the AML/CFT Law should be established between the need to ascertain whether a customer is acting on behalf of another person and the requirement to collect identification data. Further clarification in the AML/CFT Law on the meaning of the term “beneficiary” and the measures which financial institutions should take to comply with the measures would be helpful. • Further guidance to FIs should be developed to ensure that legal arrangements are appropriately identified as the financial sector grows and becomes more international. *Recommendation 6* • Further guidance should be given as to the requirements for dealing with existing customers who are found to be foreign public persons, establishing the source of wealth and conducting enhanced ongoing due diligence. Also, the measures should extend to beneficial owners. Russia should also consider extending the provisions to include domestic PEPs. *Recommendation 7* • All of the relevant criteria should be set out in law, regulation or other enforceable means, particularly the need to understand the nature of the respondent bank’s business and to ascertain whether the respondent’s AML/CFT system is adequate and effective. The requirement to document the respective AML/CFT responsibilities of banks should also be covered, and Russia should consider formalising its requirements in relation to payable-through accounts. *Recommendation 8* • Russia should review the existing limited requirements (which relate largely to remote banking) and to provide appropriate measures on the basis of that review.
3.3 Third parties and introduced business (R.9)	• Russia should amend the AML/CFT Law to state clearly that financial institutions are not permitted to rely on third party verification of identity.
3.4 Financial institution secrecy or confidentiality (R.4)	• Russia should address the uncertainty regarding the definition of “authorised body” in the AML/CFT Law to ensure that all supervisors are covered.

Recommended Action	
3.5 Record keeping and wire transfer rules (R.10 & SR.VII)	*Recommendation 10* • Russia should address the gaps in the legal regime for record keeping. • Russia should update the AML/CFT Law to include all necessary record keeping requirements, even if this duplicates requirements set out in other laws. *Special Recommendation VII* • Russia should amend the current AML/CFT regime to address the following deficiencies *i)* the definition of originator information may well be sufficient in the context of the Russian payment system framework, but it does not fully cover all requirements set by the FATF, *ii)* incoming cross-border wire transfers are not covered by a requirement to adopt effective risk based procedures for incomplete originator information, and this vulnerability is not mitigated by the argument (as provided by the authorities) that most incoming cross-border wire transfers originate in countries that are largely compliant with FATF recommendations, *iii)* the BoR should provide specific guidance to credit institutions regarding the application of wire transfer regulations to batch transfers, *iv)* Russia should develop rules requiring financial institutions to apply a risk-based procedure for wire transfers that lack full originator information, and *v)* as a matter of effective implementation, if Russia amends the current law to include incoming cross-border wire transfers, Russian authorities will need to reconsider the current blanket requirement to simply refuse all transactions without full originator information as this could theoretically result in a complete halt to all incoming cross-border wire transactions.
3.6 Monitoring of transactions and relationships (R.11 & 21)	*Recommendation 11* • Russia should require FIs to examine as far as possible the background and purpose of all unusual transactions and to set forth the findings of such examinations in writing and to keep such findings available for competent authorities and auditors for at least five years. Russia should additionally make sure that FIs are no longer confused about the distinction between mandatory threshold reporting (> RUB 600 000) and examining the background of unusual transactions. Also, Russia should provide more guidance to the FIs, especially to make clear that the types of unusual transactions listed in laws and regulations are neither exhaustive nor closed. *Recommendation 21* • Russia should require FIs to give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF Recommendations. FIs should also examine as far as possible the background and purpose of business relationships and transactions with persons from or in those countries, to set forth the findings of such examinations in writing and to keep these findings available for competent authorities and auditors for at least five years. • Since Russia indicates it has the legal framework through the new Law on Special Economic Measures, it should use this framework to apply countermeasures, as envisaged by Recommendation 21. • As a matter of urgency, Russia should establish a set of countermeasures that it can require the FIs to take in case a country continues to disregard the FATF Recommendations.
3.7 Suspicious transaction reports and other reporting (R.13-14, 19, 25 & SR.IV)	*Recommendation 13 and Special Recommendation IV* • Russia should criminalise insider trading and market manipulation, so as to enable FIs to report STRs based on the suspicion that a transaction might involve funds generated by the required range of criminal offences. • Russia should finally introduce a reporting obligation for attempted transactions by occasional customers. • Russia should issue TF guidance to enhance the effectiveness of the system for filing TF STRs • Russia should raise the awareness in the non-CI FIs, at a minimum through an enhanced training programme. The training should not only focus on the legal obligations, but also include the reasons for establishing an AML/CFT system, as well as examples, typologies and cases. *Recommendation 14* • Russia should extend the safe harbour provision and the tipping off prohibition to the FIs and their directors.

Recommended Action	
	Recommendation 25 • Russia should extend the case by case feedback beyond the acknowledgement of the receipt of the STR. It should also urgently consider other examples of case-by-case feedback, as those examples listed in the FATF Best Practice Paper for feedback by FIUs.
3.8 Internal controls, compliance, audit and foreign branches (R.15 & 22)	*Recommendation 15* • The Russian authorities should ensure that all FIs establish and maintain internal procedures, policies and controls to manage both AML/CFT and prudential risks, and to ensure that these policies and procedures are comprehensively communicated to all relevant employees. Financial institutions and supervisory bodies should also ensure that training programmes incorporate case studies and other practical demonstrations of both money laundering and terrorism financing so employees are better able to detect signs of ML and FT when they occur. With respect to terrorism financing, FIs and supervisory bodies should amend internal control programme requirements to incorporate a more comprehensive approach to CFT beyond the current practice of simply checking the list of designated entities. • The Russian authorities should enhance existing provisions regarding employee screening procedures to ensure that all employees of FIs can be sufficiently screened. Screening procedures should take criminal records into account, but should also assess the vulnerability to corruption of each employee or group of employees. • ROSCOM and Russia Post should take proactive and comprehensive steps to ensure that all employees at all branches of Russia Post across the country have a good understanding of the Post's internal control programmes with respect to AML/CFT requirements of the ICP, and that compliance units are sufficiently trained and fully implementing all legal and regulatory requirements related to AML/CFT. The Russian authorities should work closely with Russia Post to ensure that the independent audit programme is being carried out effectively and comprehensively at all branches to verify compliance with internal control requirements across the country. *Recommendation 22* • The Russian authorities should consider harmonising the existing legal and regulatory framework to ensure that all foreign operations – both branches and subsidiaries – of Russian FIs observe Russian AML/CFT requirements. Existing guidance for credit institutions on managing the risk associated with foreign operations should be expanded to address ML and TF risks as well as prudential risks. Russian regulators should consider issuing specific guidance to Russian credit institutions regarding the need for increased vigilance over foreign operations in jurisdictions that do not (or insufficiently) apply the FATF recommendations. FIs should be required to inform its Russian supervisor when a foreign operation is unable to observe appropriate AML/CFT measures because of local conditions.
3.9 Shell banks (R.18)	No recommendations.
3.10 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	*Recommendation 23 / banking sector* • Russia should – as a matter of urgency – strengthen the regime to prevent criminals from becoming major shareholders in a CI by amending the Banking Law to lower the threshold from 20% to 10%, by ensuring that every person who, directly or indirectly, holds more than 10% of the shares or the votes of a credit institution, is checked as a major shareholder and by ensuring that the BoR can refuse an acquisition if the concerned person was convicted for having committed a financial crime. *Recommendation 23 / other sectors* • Russia should as a matter of urgency – and as already recommended in the Second Round Evaluation Report by MONEYVAL – *i)* implement provisions to prevent criminals from becoming major shareholders in a non-CI FI, *ii)* raise the awareness of the staff of the FSFM, the FISS and ROSCOM and increase their number of staff substantially to ensure that every FI undergoes at least one on-site inspection every three years and that – on a risk basis - more targeted in-depth thematic reviews are carried out, and *iii)* consolidate and strengthen the system to register and supervise organisations providing MVT services according to article 13.1 Banking Law, including the implementation of fit and proper tests. • Russia should implement fit and proper tests for leasing companies and amend the Insurance Law to ensure that members of the board of a life insurance company or an insurance broker are fit and proper.

Recommended Action	
	• Russia should amend the Law on Communications to ensure that all conceivable money and value transfer service providers are licensed or registered and supervised. *Recommendation 29 / banking sector* • Russia should amend the BoR Law to elevate the maximum amount for fines against credit institutions substantively and to ensure that the BoR has the competence to impose adequate fines on directors and senior management of banks for violation of AML/CFT requirements. • Russia should amend the BoR Law to ensure that a licence of a CI can be revoked when the owners are convicted off a relevant criminal or economic offences and to ensure that a licence of a CI can also be revoked for not filing STRs with the FIU. Russia should also ensure that the licence of a CI can be revoked not only if repeated violations occur during one year and thus, amend the BoR Law accordingly. • Russia should abolish the limitation of the BoR to conduct on-site inspections in article 73 item 5 BoR Law, as already recommended in the MONEYVAL Second Round Report. *Recommendation 29 / other sectors* • Russia should – as a matter of urgency (i) amend the relevant laws to ensure that the FSFM, the FISS and ROSCOM have the power to impose fines on their FIs and on directors and senior management of their FIs for violation of AML/CFT requirements and to replace directors and senior management of their FIs for violation of AML/CFT requirements, (ii) abolish the limitation of the FISS to compel and obtain access to banking secrecy information and (iii) increase the staff for the FSFM, the FISS and ROSCOM to ensure that the system for sanctioning financial institutions works effectively. • Russia should stipulate explicitly ROSCOM's competence to carry out on-site inspections with respect to the full set of AML/CFT requirements and to compel production of records. • Russia should in addition amend the relevant laws to ensure that a licence can be revoked for violation of AML/CFT requirements also in the non-banking and non-securities sectors, and when the owners are convicted of a relevant criminal or economic offences (concerns the FSFM, the FISS, ROSCOM and Rosfinmonitoring). • Russia should amend the Law on the Securities Market to ensure that a licence of a corresponding FI can also be revoked for not filing STRs with the FIU and abolish the precondition of repeated violations during one year to revoke a licence. *Recommendation 17* • Russia should amend article 15.27 Code of Administrative Offences to ensure that the main violations of the AML/CFT Law are covered, especially regarding non compliance with the requirement to identify the customer and the beneficial owner and to elevate the maximum amount for fines against officials of financial institutions. *Recommendation 25* • Russia should implement the requirement to issue guidance to FIs, beyond the explanation of the law.
3.11 Money and value transfer services (SR.VI)	• Russia should consider implementing laws and regulations to ensure that postal operations are better aware of and in compliance with the AML/CFT requirements. Suggested improvements would include: (1) increased technical interface between postal branches to better detect suspicious transactions, (2) rules governing the volume and frequency of remittances permitted and (3) improved training of postal operators on AML/CFT. Given the size of the postal sector, Russia should also consider either increasing the capacity and quality of ROSCOM's compliance function or transferring supervisory and regulatory powers to another federal authority that is better equipped and trained to assess AML/CFT compliance. • Russia should find ways to ensure that ROSCOM has sufficient powers to correct deficiencies found in Russia Post's AML/CFT compliance. • Russian law enforcement bodies should place a higher priority on investigating the existence of alternative remittance systems to better assess the size and the nature of ML/TF threat posed by illegal MVT occurring within and through Russia.
Section 4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due	• Russia should review the AML/CFT regime as it applies to DNFBPs and ensure that all

Recommended Action	
diligence and record-keeping (R.12)	of the relevant criteria are addressed. For casinos, real estate agents and dealers in precious metals and stones, the basic recommendations set out earlier in this report in relation to Recommendations 5, 6 and 8-11 are applicable, as these entities are subject to the full effect of the AML/CFT Law in Russia. • In relation to lawyers, accountants and notaries, specific provisions to address all of the relevant criteria in Recommendations 5, 6 and 8-11 should be developed. In particular, extending the CDD requirements to include their full range in the legislation. Russia should also take steps to examine ways of increasing the effectiveness of compliance with AML/CFT requirements in these sectors. • With a diverse range of supervisory bodies (Rosfinmonitoring, the Assay Chamber, the Federal Notaries Chamber and the Federal Lawyers Chamber) Russia should take steps to co-ordinate the overall approach in this area. • Russia should also examine the use of cash in the real estate sector in order to be sure that there are no important gaps in the AML/CFT system as it relates to this sector.
4.2 Suspicious transaction reporting (R.16)	• Russia should take steps to ensure that all institutions covered by the requirement to report STRs are aware of the difference between these reports and those relating to mandatory control. • For lawyers, notaries and accountants, Russia should take steps to improve understanding of the requirements in this area, given the current low level of reporting, and the lack of information available to evaluate the effectiveness of the regime. • The authorities should continue working with lawyers, notaries and accountants to ensure full compliance with the requirements relating to internal controls. • Russia should take further steps to ensure that covered institutions are aware of the need to pay special attention to customers from countries that do not sufficiently apply the FATF Recommendations.
4.3 Regulation, supervision and monitoring (R.24-25)	• Russia should improve the data available to analyse the effectiveness of the measures it is taking. Rosfinmonitoring should consider introducing a greater element of risk-based supervision in relation to the categories of firms it supervises. In particular, the risks identified by Rosfinmonitoring in relation to casinos should be subject to greater supervisory attention. • The role of real estate agents should be examined to ensure that no gaps exist in the AML/CFT system. In particular, the contention that most flows of funds in real estate transactions are routed through the banking sector should be verified, and the level of risk relative to the supervisory activity of Rosfinmonitoring in this area should be considered. • The system for supervising lawyers' and notaries' compliance with the AML/CFT Law should be enhanced considerably. • The current regime for licensing casinos will not change until 30 June 2009 (see section 1). In the meantime Russia should consider how it will implement this change and develop plans to deal with unlicensed gambling. The current and future regime contains no specific provision to prevent criminals or their associates from holding an interest in a casino. This should be addressed. • The Assay Chamber should have more specialist AML/CFT staff in order to better perform its functions. • Consideration should also be given to the Assay Chamber's suggestion that supervisors be given greater access to the content of STRs in order to better target supervisory action. • Russia should take further steps to strengthen the AML/CFT supervisory regime for accountants.
4.4 Other non-financial businesses and professions (R.20)	• Russia should consider the ML risk posed by the proliferation of high value and luxury goods providers in Moscow and other major urban centres that has accompanied Russia's recent oil boom. • Russia should seek to continue reducing its reliance on cash and introduce more efficient payment systems that have also been introduced in other countries around the world. Adopting more modern payment techniques should also reduce the need for high denomination bank notes.

Recommended Action	
Section 5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal Persons – Access to beneficial ownership and control information (R.33)	• The Russian authorities should implement a system that requires adequate transparency regarding the beneficial ownership and control of legal persons.
5.2 Legal Arrangements – Access to beneficial ownership and control information (R.34)	• No recommendations.
5.3 Non-profit organisations (SR.VIII)	• Russia should undertake a comprehensive review of the NPO system, as foreseen by Special Recommendation VIII. • Russia should reach out to and engage with the NPO sector, to learn from the sector, to promote values and the like. • The Russian authorities should set up a more formalised and efficient system that focuses on potential vulnerabilities and to share information to target abuse. • Existing rules should be fully implemented.
Section 6. National and International Co-operation	
6.1 National co-operation and co-ordination (R.31)	• Russia should ensure that the outcome of policy reviews are implemented, especially in areas that are not the responsibility of Rosfinmonitoring. • Russia should make an extra effort to enhance operational-level co-operation among law enforcement agencies, and between law enforcement and supervisory authorities to sharpen Russia's focus on the possible existence of illegal alternative remittance systems within Russia. This effort should aim to develop a sense of the threat as well as a prescription for addressing the problem.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• Russia should correct the deficiencies noted in relation to the implementation of the relevant international conventions and UNSCRs as soon as possible. Russia should also institute criminal liability for legal persons. • Russia should implement the provisions of UNSCRs 1267, 1373 and successor resolutions.
6.3 Mutual Legal Assistance (R.36-38 & SR.V)	• Russian authorities should continue to institute a pro-active approach to monitoring progress on execution of requests and better ensuring a timely and effective response. • The General Prosecutor's Office should ensure that clear lines of communication exist with established points of contact between itself and the law enforcement officer responsible for execution of the request, as well as between itself and the requesting country. • The authorities should maintain statistics on the more detailed aspects of MLA including details on the nature and results of MLA requests. • The Russian authorities are encouraged to continue their monitoring of the process of providing MLA among special MLA working groups established with a number of countries.
6.4 Extradition (R.39, 37 & SR.V)	• Russia should further enhance the existing system of reviews in relation to extradition according to Instruction No. 32/35 and maintain comprehensive statistics in relation to ML/TF covering all details of the extradition process. • Russia should also raise the effectiveness of its extradition practice in relation to non-CIS countries and make the figures for CIS and non-CIS countries better comparable. Russia is however to be commended for the high number of requests to and from CIS countries. • Russia should address the missing elements of its ML and TF offences to ensure that dual criminality requirements do not represent an obstacle for extradition in such matters (see also sections 2.1 and 2.2 for discussion of the missing elements of the ML and TF offences).
6.5 Other Forms of Co-operation (R.40 & SR.V)	• No recommendations.

Recommended Action	
Section 7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	• See recommendations relating to other recommendations.
7.2 Other relevant AML/CFT measures or issues	• No recommendations.
7.3 General framework – structural issues	• No recommendations.

ANNEXES

ANNEX 1: ACRONYMS AND ABBREVIATIONS

AML	Anti Money Laundering
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
BoR	Bank of Russia
CC	Criminal Code
CDD	Customer Due Diligence
CFD	Central Federal District (Moscow)
CFT	Combating the Financing of Terrorism
CCP	Code of Criminal Procedure
CCRL	Currency Control and Regulation Law
CI	Credit Institution
DNFBP	Designated Non-Financial Businesses and Professions
EAG	Eurasian Group
EUR	Euro (currency)
FATF	Financial Action Task Force
FCS	Federal Customs Service
FEFD	Far East Federal District (Khabarovsk)
FI	Financial Institution
FISS	Federal Insurance Supervision Service
FIU	Financial Intelligence Unit
FSKN	Federal Service for the Control of Narcotics Circulation
FSFM	Federal Service for Financial Markets
FT	Financing of Terrorism
FTS	Federal Tax Service
ID	Identification
MFA	Ministry of Foreign Affairs
MIA	Ministry of Internal Affairs
ML	Money Laundering
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
MoF	Ministry of Finance
MoJ	Ministry of Justice
MOU	Memorandum of Understanding
MVT	money or value transfer
NASP	National AML/CFT Strategy Paper
NPO	non-profit organisation
NWFD	North West Federal District (Saint Petersburg)
Palermo Convention	United Nations Convention against Transnational Organised Crime
PEP	Politically Exposed Person
ROSCOM	Roscommunication (Rossvyazokhrankultura)
ROSREG	Rosregistration (Federal Registration Service)
RUB	Russian Rouble (currency)
SFD	Southern Federal District (Rostov-na-Donu)
SiFD	Siberian Federal District (Novosibirsk)
STR	Suspicious Transaction Report
TF	Terrorist Financing
TF Convention	International Convention for the Suppression of the Financing of Terrorism
UFD	Ural Federal District (Yekaterinburg)
UN	United Nations
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution
USD	United States Dollar (currency)
USRLE	Unified Central Registration System
VFD	Volga Federal District
Vienna Convention	United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances

ANNEX 2 - LIST OF GOVERNMENT AND PRIVATE SECTOR BODIES INTERVIEWED (FOR EACH PLACE IN ALPHABETIC ORDER)

1. Mr V. Zubkov, Chairman of Government of the Russian Federation
2. Mr V. Ivanov, Assistant to the President of the Russian Federation
3. Mr A. Kudrin, Deputy Prime Minister and Minister of Finance of the Russian Federation
4. Mr V. Lebedev, President of the Supreme Court of the Russian Federation
5. Mr R. Nurgaliev, Minister of Internal Affairs of the Russian Federation

Moscow

6. Rosfinmonitoring (headquarters)
7. Alpha Bank
8. Association of Russian Banks
9. Bank of Russia (headquarters)
10. Club Europa Casino
11. Federal Customs Service (headquarters)
12. Federal Insurance Supervision Service (headquarters)
13. Federal Lawyers Chamber (headquarters)
14. Federal Notarial Chamber (headquarters)
15. Federal Security Service (FSB) (headquarters)
16. Federal Service for Financial Markets (headquarters)
17. Federal Service for the Control of Narcotics Circulation (headquarters)
18. Federal Tax Service (headquarters)
19. General Prosecution Office (headquarters)
20. Ingosstrakh (Insurance)
21. Ministry of Foreign Affairs (headquarters)
22. Ministry of Internal Affairs (headquarters)
23. Ministry of Justice (headquarters)
24. Raiffeisenbank Austria
25. Renaissance Broker Securities Company
26. Rosfinmonitoring Central Federal District regional office
27. Rosfinmonitoring North West Federal District regional office
28. Rosfinmonitoring Siberia Federal District regional office
29. Rosfinmonitoring Ural Federal District regional office
30. Russia Post Moscow District Office
31. Savings Bank (Sberbank)
32. Sobinbank
33. State Assay Chamber (headquarters)
34. Supreme Court of Russia (headquarters)
35. Trading House of Vinogradova
36. Vozrozhdenie Bank

Nizhniy Novgorod

37. Rosfinmonitoring Volga Federal District regional office
38. Alexandrovsly Garden Country Casino
39. Aviva Insurance
40. Bank of Russia Nizhniy Novgorod District
41. Bank of Russia Volga Federal District
42. Federal Customs Service Volga Federal District
43. Federal Insurance Supervision Service Volga Federal District
44. Federal Security Service (FSB) Volga Federal District
45. Federal Service for Financial Markets Volga Federal District
46. Federal Service for the Control of Narcotics Circulation Volga Federal District
47. Forum Bank
48. General Federal District Court Volga Federal District
49. Ministry of Internal Affairs Academy
50. Ministry of Internal Affairs Volga Federal District
51. Prosecution Authority Volga Federal District
52. Roscommunications Volga Federal District
53. Rosprocat Leasing

Khabarovsk

54. Rosfinmonitoring Far East Federal District regional office
55. Bank of Russia Far East Federal District
56. Dalgaso Insurance
57. Dalkombank
58. Federal Customs Service Far East Federal District
59. Federal Insurance Supervision Service Far East Federal District
60. Federal Security Service (FSB) Far East Federal District
61. Federal Service for Financial Markets Far East Federal District
62. Federal Service for the Control of Narcotics Circulation Far East Federal District
63. Federal Service for the Control of Narcotics Circulation Khabarovsk Krai
64. General Federal District Court Khabarovsk
65. Ministry of Internal Affairs Far East Federal District
66. Nadjima Casino
67. Prosecution Authority Far East Federal District
68. Regional Bureau of Real Estate

69. Roscommunications Far East Federal District
70. Russia Post Far East Federal District
71. State Assay Chamber Far East Federal District

Kaliningrad

72. Rosfinmonitoring North West Federal District
73. Aini Insurance
74. Almazholding Precious Stones
75. AVK Securities
76. Bank of Russia North West Federal District
77. Don Quichote Casino
78. Europejskiy Bank
79. Federal Customs Service Kaliningrad Oblast
80. Federal Customs Service North West Federal District
81. Federal Insurance Supervision Service North West Federal District
82. Federal Security Service (FSB) North West Federal District
83. Federal Service for Financial Markets North West Federal District
84. Federal Service for the Control of Narcotics Circulation North West Federal District
85. General Federal District Court North West Federal District
86. Ministry of Internal Affairs Kaliningrad District
87. Ministry of Internal Affairs Transportation Department Kaliningrad District
88. Prosecution Authority Kaliningrad Oblast
89. Roscommunications North West Federal District
90. State Assay Chamber North West Federal District

Rostov-na-Donu

91. Rosfinmonitoring South Federal District regional office
92. Bank of Russia Rostov District
93. Federal Customs Service Rostov District
94. Federal Customs Service Southern Bureau
95. Federal Insurance Supervision Service South Federal District
96. Federal Security Service (FSB) Rostov District
97. Federal Service for Financial Markets South Federal District
98. Federal Service for the Control of Narcotics Circulation Rostov District
99. Federal Service for the Control of Narcotics Circulation South Federal District
100. General Federal District Court Rostov
101. LLC Alfa-Don Real Estate Center
102. Ministry of Internal Affairs North Caucasian Office
103. Ministry of Internal Affairs Novocherkassk
104. Ministry of Internal Affairs Rostov District
105. Ministry of Internal Affairs South Federal District
106. OJSC MeTraComBank
107. Partner Securities
108. Prosecution Authority Rostov
109. Prosecution Authority South Federal District
110. Roscommunications Rostov District
111. Russia Post Rostov District
112. State Assay Chamber Don District

ANNEX 3: KEY LAWS, REGULATIONS AND OTHER MEASURES

AML/CFT Law

Federal Law of August 7, 2001 No. 115-FZ – «On Combating Legalisation (Laundering) of Proceeds from Crime and Financing of Terrorism» (with changes according to Federal laws No. 112-FZ dated July 25.07.2002, No. 131-FZ dated 30.10.2002, No. 88-FZ dated 28.07.2004, No. 145-FZ dated 16.11.2005, No. 147-FZ dated 27.07.2006, No. 153-FZ dated 27.07.2006, No. 51-FZ dated 12.04.2007, No. 197-FZ dated 19.07.2007, No. 214-FZ dated 24.07.2007, No. 275-FZ dated 28.11.2007)

Chapter I. General Provisions

Article 1. Goals of the present Federal law

The present Federal law shall be aimed at the protection of the rights and legal interests of citizens, society and state by means of creation of the legal mechanism of taking actions against legalisation (laundering) of proceeds from crime and financing of terrorism.

Article 2. Sphere of application of the present Federal law

The present Federal law shall regulate relationships of citizens of Russia, foreign citizens and persons without citizenship, organisations performing operations with monetary funds or other assets, as well as state authorities performing control on the territory of Russia over performance of operations with monetary funds or other assets, for purposes of prevention, revelation and curbing of actions connected with legalisation (laundering) of proceeds from crime, and financing of terrorism. In accordance with international agreements of Russia this Federal law shall be applied to persons and legal entities performing operations with monetary funds or other assets outside the territory of Russia.

Article 3. Basic concepts used in this Federal law

The following basic concepts shall be used for purposes of this Federal law: Proceeds from crime - monetary funds or other assets obtained as a result of a crime; legalisation (laundering) of proceeds from crime - making ownership, use or disposition of monetary funds or other assets obtained as a result of a crime legal, except for crimes provided by articles 193, 194, 198, 199, 199.1 and 199.2 of the Criminal Code of Russia; financing of terrorism – providing or collecting funds or rendering financial services knowing that they are aimed at financing of arrangement, preparation and commission of at least one of the crimes stipulated by articles 205, 205.1, 205.2, 206, 208, 211, 277, 278, 279 and 360 of the Criminal Code of Russia, or at supporting an organised group, illegal armed formation, or criminal association (criminal organisation) established or being established for committing at least one of the mentioned crimes; operations with monetary funds or other assets - operations of persons and legal entities with monetary funds or other assets regardless of the form and way of performance thereof, directed to establishing, changing or termination of legal rights and liabilities connected therewith; authorised body - federal executive authority taking actions against legalisation (laundering) of proceeds from crime, and financing of terrorism in accordance with this Federal law; obligatory control - combination of measures taken by the authorised body for control over operations with monetary funds or other assets on the basis of the information provided thereto by organisations performing these operations, as well as for verification of this information in accordance with the legislation of Russia; internal control - activity of organisations performing operations with monetary funds or other assets for revealing operations to be put under obligatory control and other operations with monetary funds or other assets, connected with legalisation (laundering) of proceeds from crime, and financing of terrorism.

Chapter II. Prevention of legalisation (laundering) of proceeds from crime and financing of terrorism

Article 4. Measures taken against legalisation (laundering) of proceeds from crime and financing of terrorism

Measures taken against legalisation (laundering) of proceeds from crime and financing of terrorism shall include: Obligatory procedures of internal control; Obligatory control; Banning on informing clients and other persons on measures taken against legalisation (laundering) of proceeds from crime and financing of terrorism; Other measures taken in accordance with the federal laws.

Article 5. Organisations performing operations with monetary funds or other assets

For purposes of this federal law the following shall be related to organisations performing operations with monetary funds or other assets: Credit institutions; Professional participants of the security market; Insurance organisations and leasing companies; Organisations of federal post communication; Pawn shops; Organisations involved in purchase, buy-sell of precious metals and precious stones, jewellery made out of them and scratched items; Organisations arranging totalisators and bookmaker offices as well as organising and carrying out lotteries, totalisators (mutual bets) and other risk-based games, including in electronic form; organisations managing investment funds or non-governmental pension funds; organisations rendering intermediary services when performing operations of sale and purchase of real estate; non-credit organisations accepting cash funds from physical persons in cases provided for by the legislation on banks and banking activity; commercial organisations concluding financial contracts on cession of money rights as financial agents.

Article 6. Operations with monetary funds or other assets due to obligatory control

1 Operations with monetary funds or other assets shall be subject to obligatory control, if the amount at which it is performed equals or exceeds 600000 roubles or hard currency sum equivalent to 600.000 roubles, and by its character this operation is one of the following operations.

1) cash operations with monetary funds: withdrawal from an account or placement in an account of a legal entity of cash funds in the events which are not provided by the character of its economic activity; purchase or sale of cash foreign currency by a natural person; acquisition by a person of securities for cash; getting by a person of a bearer's check cashed, issued by a non-resident; change of notes of one denomination for notes of other denomination: contributing by a person of cash funds in the authorised capital of an organisation;

2) placement or remittance of monetary funds into an account, provision or getting of a credit (loan), operations with securities, if at least one of the sides is a person or a legal entity having registration, place of residence or location in the state (on the territory), which does not participate in the international cooperation in the sphere of combating money laundering and financing of terrorism, or one of the sides is a person which is an owner of an account in the bank registered in such state (or the territory). The list of these states (territories) shall be determined in the procedure set by the Government on the basis of lists approved by international organisations combating money laundering and financing of terrorism, and shall be subject to publication;

3) operations on bank accounts (deposits): placement of monetary funds in deposits (on deposits) with execution of documents certifying a bearer's deposit; opening of a deposit in favour of the third parties with placement therein of cash funds; remittance of monetary funds abroad onto an account (deposit) opened for an anonymous owner and incoming of monetary funds from abroad from an account (deposit) opened for an anonymous owner; placement of monetary funds into an account (deposit) or withdrawal from an account (deposit) of a legal entity whose term of activity does not exceed three months from the date of its registration, or placement of monetary funds into an account (deposit) or withdrawal from an account (deposit) of a legal entity in case no operations have been performed on this account (deposit) since the date of opening thereof;

4) other operations with movable property: placement of precious metals, precious stones, jewellery made out of them and scratched items or other valuables into pawn shop; payment of an insurance indemnity to a person or receiving from him of an insurance premium for life insurance or other types of accumulation insurance and pension allowance; obtaining or providing property under contract of financial leasing; remittance of monetary funds performed by non-credit institutions by client's order; purchase, buy-sell of precious metals and precious stones, jewellery items made of them and scratched items; receiving monetary funds as payment for participation in a lottery, totalisator (mutual bet) and other risk-based games, including in electronic form, and payment of monetary funds as the prize received from participation in these games; granting by the legal persons that are not credit organisations, of interest-free loans to natural persons and (or) to other legal persons, as well as reception of such loan.

1.1. Operations with real estate is subject to the obligatory control if the amount of it is equal to or exceeds 3000000 roubles or is equal to or exceeds the amount in a foreign currency equivalent to 3000000 roubles.

2. Operation with monetary funds or other assets is subject to obligatory control when at least one of the sides is an entity or a person on which there are data received in procedure set by the present Federal law about their involvement in extremist activity or terrorism, or a legal entity directly or indirectly owned or under control of such organisations or persons, or a person or entity acting in the name or by order of such entity or person. The procedure of determining and disseminating the list of such entities and persons to organisations performing operations with monetary funds or other assets, is set by the Government. An entity or a person is to be included into the mentioned list on following basis: A Russian Federation court decision entered into legal force on liquidation or prohibition of activity of organisation in connection with its involvement in extremist activity or terrorism; A Russian Federation court sentence entered into legal force on declaring a person guilty in committing a terrorist crime; A decision of the Prosecutor General or a subordinate to him prosecutor on suspending activity of an organisation in connection with their claim to the court to draw the organisation to liability for terrorist activity; Order by an investigator for initiating a criminal case concerning a person having committed a terrorist crime; Lists of entities and persons connected to terrorist organisations or terrorists set by international organisations fighting against terrorism or by authorised by them bodies and accepted by Russia; Accepted by Russia in accordance with international agreements of Russia and federal laws sentences (decisions) of courts and other competent authorities of foreign states on organisations or persons performing terrorist activity; Inclusion of an organisation in accordance with Federal law No. 35-FZ dated March 6, 2006 “On combating terrorism” into the federal list of organisations, including foreign and international organisations, recognised by the courts of Russia as terrorist organisations.

3. In case an operation with funds or other property is carried out in foreign currency, its equivalent sum in Russian roubles is set by the exchange rate of the Central Bank valid on the day that this operation was conducted.

4. Reports on operations with monetary funds or other assets due to obligatory control are submitted directly to the authorised agency by institutions performing operations with monetary funds or other assets.

Article 7. Rights and responsibilities of organisations performing operations with monetary funds and other assets

1. Organisations performing operations with monetary funds and other assets are obliged to:

1) identify the person serviced by the organisation performing operations with monetary funds or other assets (client), excluding cases established by items 1.1. and 1.2. of the present article, and establish the following data: regarding natural persons - a surname, a name,

and also a patronymic (if other does not follow from the law or national custom), citizenship, data of the document certifying the person, the data of a migration card, the document confirming the right of the foreign citizen or the person without citizenship on stay (residing) in Russia, the address of residence (registration) or a place of stay, taxpayer's identification number (at its presence); regarding legal persons - the name, taxpayer's identification number or a code of the foreign organisation, state registration number, a place of the state registration and the address of location;

2) undertake reasonable and accessible in the specific circumstances measures for establishment and identification of beneficiaries, except in cases established by items 1.1.and 1.2 of the present article;

3) regularly update the information on clients, beneficiaries;

4) to fix in documents and submit to the authorised body the following information on operations with monetary funds or other assets which are subject to obligatory control, not later than the working day following the date of performance of the operation: the type of operation and grounds for performance thereof; the date of performance of the operation with monetary funds or other assets, as well as the amount at which it was performed; information necessary for identification of the person who performs operations with monetary funds or other assets (data of the passport or another identification card), the data of a migration card, the data of the document confirming the right of the foreign citizen or the person without citizenship on stay (residing) in Russia, taxpayer's identification number (if it exists), the address of his residence or a place of stay; the name, taxpayer's identification number, state registration number, place of state registration and the address of the location of the legal entity, which performs the operation with monetary funds or other assets; information necessary for identification of a person or legal entity by whose order and on whose behalf an operation with monetary funds or other assets is performed, the data of a migration card, the data of the document confirming the right of the foreign citizen or the person without citizenship on stay (residing) in Russia, taxpayer's identification number (if it exists), residential address or address of the place of location correspondingly of the person or legal entity; the information necessary for identification of the representative of the natural or legal person, the attorney, the agent, the commission agent, the trustee performing operation with monetary funds or other assets, on behalf of or in interest of or at expense of other person by virtue of the power based on proxy, the contract, the law or the certificate of the authorised state body or institution of local self-management, the data of a migration card, the data of the document confirming the right of the foreign citizen or the person without citizenship on stay (residing) in Russia, taxpayer's identification number (at its presence), the address of a residence of the representative of the natural or legal person; the information necessary for identification of the addressee on operation with monetary funds or other assets and his representative, including the data of a migration card and the document confirming the right of the foreign citizen or the person without citizenship on stay (residing) in Russia, taxpayer's identification number (at its presence), the address of a residence or a site of the addressee and his representative if it is stipulated by rules of performance of corresponding operation;

5) to submit to the authorised body, upon its written requests, information stated in sub item 4 of this clause both with respect to operations which are subject to obligatory control and operations stated in sub item 3 of this article. The procedure of submission by the authorised body of the above mentioned requests shall be determined by the Government as agreed with the Bank of Russia. The authorised body shall not have the right to ask for documents and information on operations performed before the enforcement of this Federal law, except the documents and information which shall be submitted on the basis of the appropriate international agreement of Russia.

1.1. Identification of the client – natural person, verification and identification of the beneficiary are not performed when organisations performing operations with funds or other assets carry out operations for accepting from clients – natural persons of the following payments if they do not exceed 30000 roubles or an amount in foreign currency equivalent to 30000 roubles:

1) related to settlements with budgets of all levels of the budget system of Russia (including federal, regional and local taxes and duties, as well as fines those provided for by the legislation of Russia on taxes and duties);

2) related to payment for services rendered by budget institutions being under management of federal executive bodies, executive bodies of the constituent entities of Russia and bodies of local self-management;

3) related to payment for flats, communal services, payment for safeguarding flats and instalment of safeguarding signalisation, as well as payment for communications services;

4) related to payment of contributions by members of orchid, garden, summer houses' non-commercial associations of citizens, garage-construction cooperatives. Payments for paid auto placements;

5) related to payments of alimony.

1.2. At carrying out by a natural person of an operation on buying or selling cash foreign currency for the amount not exceeding 15000 roubles or not exceeding the amount in foreign currency equivalent to 15000 roubles, the identification of the client – natural person, verification and identification of beneficiary are not performed except the case when an officer of the organisation performing operations with monetary funds or other assets has suspicion that this operation is carried out with the aim of legalisation (laundering) of proceeds from crime or financing of terrorism.

1.3 Organisations carrying out operations with monetary funds or other assets, in addition to the measures stipulated by item 1 of the present Article shall be obliged to:

1) adopt reasonable and possible in the circumstances measures on identification, among physical persons serviced or when establishing business relations, of foreign public persons;
2) establish business relations with foreign public persons only upon written approval of the head of the organisation carrying out operations with monetary funds or other assets, or his deputy;
3) take reasonable and possible in the circumstances measures to establish the source of the monetary funds or other assets of foreign public persons;
4) update on the permanent basis the information the organisation carrying out operations with monetary funds or other assets has, on the foreign public persons serviced by them;
5) pay higher attention to the operations with monetary funds or other assets performed by foreign public persons, their spouses, close relatives (direct relatives (parents and children, grandparents and grandchildren), full blood and half-blood (having common father or mother) brothers and sisters, the adopters and the adopted) or on behalf of those persons.

2. In order to prevent legalisation (laundering) of proceeds from crime and financing of terrorism, organisations performing operations with monetary funds or other assets must develop rules of internal control and programmes of its performance, appoint officials responsible for the observance of these rules and realisation of these programmes, as well as take other internal organisational measures for the indicated purposes. Rules of internal control of an organisation performing operations with monetary funds or other assets must include the procedure for fixing of the necessary information in documents, procedure for provision of confidentiality of information, qualification requirements to preparation and training of the staff, as well as criteria of revealing and signs of unusual deals with the account of specific features of the activity of this organisation. In accordance with the rules of internal control, organisation performing operations with monetary funds or other assets must fix in documents the information obtained as a result of application of these rules and realisation of the programmes of internal control, and preserve its confidential character. The following shall be the grounds for fixing the necessary information in documents: Intricate or unusual character of a deal which does not have evident economic sense or evident legal purpose; Incompliance of the deal with the goals of the organisation, established by founding documents of this organisation; Repeated performance of operations or deals whose character makes us suppose that the purpose for their performance is evasion of procedures of the obligatory control, provided by this Federal law; Other circumstances, which give reasons to suppose that deals are performed for purposes of legalisation (laundering) of proceeds from crime, or financing of terrorism. Internal control rules are developed with consideration of recommendations adopted by the Government, and for credit institutions – by the Bank of Russia as agreed with the authorised body, and are approved according to the procedure set by the Government. Qualifying requirements for special officials responsible for observance of rules of the internal control and programmes of its implementation, as well as requirements for education and training of the staff, for identification of clients, beneficiaries shall be determined according to the procedure established by the Government, for the credit organisations – by the Bank of Russia as agreed with the authorised body. The requirements for identification can differ depending on a degree (level) of risk of performance by the client of operations with the purpose of legalisation (laundering) of proceeds from crime or financing of terrorism.

3. If employees of an organisation performing operations with monetary funds or other assets have got any suspicions resulting from realisation of the internal control programmes, stated in clause 2 of this article, that some operations are performed for purposes of legalisation (laundering) of proceeds from crime and financing of terrorism, this organisation not later than working day following the day on which such operations are detected must forward to the authorised body information on these operations regardless to whether they refer to operations provided by article 6 of this Federal law or not.

3.1. Cashless settlements and money transfers without opening an account carried out on the territory of Russia and from Russia abroad, except those mentioned in item 11 of the present Article, shall be accompanied at all stages of carrying them out with originator information and the number of his account where the account exists through indication of that information in the settlement document or otherwise. The information on the originator – physical person shall include a name, family name, patronymic (if otherwise does not follow from law or national custom), as well as taxpayer identification number (if any) or the address (registration address) or place of living, or date and place of birth. The information on the originator – legal entity shall include the name, taxpayer identification code or foreign organisation code. The organisation carrying out operations with monetary funds or other assets shall refuse to conduct the money transfer in case of absence of information mentioned in paragraphs one-three of the present item.

4. Documents containing information stated in this article, and data necessary for identification of the personality, shall be kept not less than 5 years. The specified term is calculated from the date of the termination of relations with the client.

5. The credit institutions are prohibited to: open accounts (deposits) for anonymous owners, i.e. without supply by the person or legal entity opening the account (deposit) of the documents necessary for identification thereof. Open accounts (deposits) for natural persons without personal presence of the person opening the account (deposit), or his representative; establish and maintain relations with the banks that do not have permanent control body on the territory of the states where they are registered.

5.1. Credit institutions are obliged to undertake measures directed on prevention of establishment of relations with foreign banks-respondents with regard of

which there is information, that their accounts are used by the banks which do not have permanent control body on the territory of the states where they are registered.

5.2. Credit institutions are authorised to refuse to conclude the contract of the bank account (deposit) with natural or legal person in the following cases: absence in the location of the legal person of its permanent control body, other body or person which have the right to act on behalf of the legal person without the proxy; a person or legal entity fails to submit documents certifying the data indicated in the present Article or if invalid documents are presented; there are data on the natural or legal person concerning participation in terrorist activity, received in accordance with the present Federal law.

6. Employees of organisations providing the appropriate information to the authorised body shall not have the right to inform clients of these organisations or other persons thereabout.

7. The procedure for submission of information to the authorised body shall be established by the Government, and with respect to credit institutions - by the Bank of Russia as agreed with the authorised body.

8. Submitting to the authorised authority of reports and documents by personnel of institutions performing operations with monetary funds or other assets concerning operations and for the purposes and in the procedure set by the present Federal law shall not constitute a breach of office, banking, tax, commercial secrecy and communication secrecy (in the meaning of post remittance of monetary funds).

9. Control over execution by persons and legal entities of this Federal law in the part of registration, storage and presenting of information on operations which are subject to the obligatory control as well as over organisation of internal control shall be performed by the appropriate supervisory agencies in accordance with their competence and in accordance with the procedure established by the legislation of Russia, as well as the authorised body in the event of absence of supervisory agencies in the sphere of activity of certain organisations performing operations with monetary funds or other assets. In case supervisory bodies do not exist in the sphere of certain organisations handling operations with monetary funds or other assets, such organisations are subject to registration in the authorised agency in the procedure established by the Government.

10. Organisations handling operations with monetary funds or other assets, have to adjourn such operations excluding operations on incoming monetary funds to the account of a person or entity, for two working days as of the date a client orders the operation to be completed, and not later than the working day after the stopping of the operation the information on an operation shall be sent to the authorised agency in case if at least one of the sides is an entity or a person on which there are data on their participation in terrorist activity, received in accordance with item 2 of article 6 of the present Federal law, or a legal entity is directly or indirectly owned or under control of such organisations or persons, or a person or entity acting in the name or by order of such entities or persons. In case the Resolution of the authorised agency on the operation adjournment for the additional term on the basis of Part 3, Article 8 of this Federal law does not arrive, the organisation handles operations with monetary funds or other assets upon the client's order unless other decision constraining operation completion is taken in accordance with the Russian Federation legislation.

11. Organisation handling operations with monetary funds or other assets are liable to reject a clients order for operation completion excluding operations in incoming monetary funds at the account of a person or entity, if respective documents are not submitted required for information registration in pursue to provisions of this Federal law.

12. Adjourning of operations in accordance with item 10 and refusal to perform an operation in accordance with item 11 of this article are not basis for civil-legal liability of organisations performing operations with monetary funds or other assets for breaking conditions of respective agreements.

13. The credit institutions are obliged to fix in documents and submit to the authorised body information on cases of refusal, on the basis specified in the present Article, to conclude the contract of the bank account (deposit) with natural or legal person, refusal to perform operations, within the period not later than the working day following the day of carrying out the specified actions, according to the procedure established by the Bank of Russia as agreed with the Government.

Article 7.1. Rights and responsibilities of other persons

1. Requirements regarding identification of clients, establishment of the internal control rules, fixation and keeping of the information established by sub item 1 of item 1, items 2 and 4 of Article 7 of the present Federal law, cover lawyers, notaries and the persons carrying out business activity in the sphere of providing legal or accounting services, in cases when they prepare or carry out in the name of or on behalf of the client, the following operations with monetary funds or other assets: operations with real estate; management of client's monetary funds, securities or other assets; management of bank, savings or securities accounts; organisation of contributions for the creation, operation or management of companies; creation, operation or management of legal persons, as well as buying and selling of companies.

2. When the lawyer, the notary, the person carrying out business activity in the sphere of providing legal or accounting services, have any reasons to believe that operations or financial operations specified in item 1 of present Article, are performed or can be performed with the purpose of legalisation (laundering) of proceeds from crime or financing of terrorism, they are obliged to notify the authorised body. The lawyer and the notary have the right to submit such information both independently and through corresponding lawyer's and notary's chambers if such chambers have concluded agreements on cooperation with the authorised body.

3. The procedure of submission by lawyers, notaries, the persons carrying out business activity in the

sphere of providing legal or accounting services, of information on operations or the financial operations specified in item 2 of present Article, shall be established by the Government.

4. The lawyer and lawyer's chamber, the notary and notary's chamber, the persons carrying out business activity in the sphere of providing legal or accounting services, have no right to disclose the fact of submission to the authorised body of the information specified in item 2 of present Article.

5. The provisions of item 2 of present Article do not apply to the information subject to the requirements of the legislation of Russia for lawyer's secrecy.

Chapter III. Organisation of activities against legalisation (laundering) of proceeds from crime and financing of terrorism

Article 8. Authorised body

The authorised body established by the President of Russia is a federal executive authority whose tasks, functions and competence in the sphere of combating legalisation (laundering) of proceeds from crime and financing of terrorism are set in accordance with this Federal law. In case there are sufficient grounds demonstrating that an operation or deal are connected with legalisation (laundering) of proceeds from crime, or financing of terrorism, the authorised body shall forward the appropriate information and materials to law enforcement bodies in accordance with their competence. An authorised agency issues an order on adjourning the operations with monetary funds or other assets up to 5 days period as indicated in Item 2 Article 6 of this Federal law, in case information submitted in accordance with Item 10, Article 7 of this Federal law, by the results of preliminary checks is regarded as substantiated. In execution of this Federal law employees of the authorised body shall provide safety of the information, which became known to them, connected with the activity of the authorised body and representing official, bank, tax, commercial secrets and communication secrecy (in part of remittance of monetary funds), and shall bear responsibility for disclosure of this information, established by the legislation of Russia. Damage inflicted on persons or legal entities by illegal actions of the authorised body or its employees in connection with the performance of their functions shall be subject to compensation for the account of federal budgetary funds in accordance with the legislation of Russia.

Article 9. Presentation of information and documents

State authorities of Russia, state authorities of constituent entities of Russia and local self-management bodies shall supply to the authorised body information and documents necessary for performance of its functions (except information on citizens' private life) in accordance with the procedure established by the Government. The Bank of Russia shall supply to the authorised body information and documents necessary for performance of its functions in accordance with the procedure coordinated by the Bank of Russia. Provision of information and documents at the request of the authorised body by state authorities of Russia, state authorities of constituent entities of Russia, local self-management bodies and the Bank of Russia for purposes and in accordance with the procedure provided by this Federal law shall not be violation of official, bank, tax, commercial secrets and communication secrecy (in part of remittance of monetary funds). Provisions of this article do not apply to the information and documents which according to articles 6, 7 of the present Federal law can not be requested by the authorised agency from organisations performing operations with monetary funds or other assets or must be presented by these organisations directly to the authorised agency. Federal executive bodies, within their competence and according to the procedure agreed by them with corresponding supervisory bodies, submit to the organisations performing operations with monetary funds or other assets, the information contained in the uniform state register of legal persons, the summary state register of accredited on territory of Russia branches of the foreign companies, as well as the information on the lost, void passports, on passports of died natural persons, on the lost passport forms.

Chapter IV. International cooperation in the sphere of struggle with legalisation (laundering) of proceeds from crime and financing of terrorism

Article 10. Information exchange and legal assistance

State authorities of Russia performing activities connected with prevention of legalisation (laundering) of proceeds from crime and financing of terrorism, in accordance with international agreements of Russia, shall have cooperation with competent bodies of foreign states at the stages of information collection, preliminary investigation, litigation and execution of verdicts. The authorised body and other state authorities of Russia performing activities connected with prevention of legalisation (laundering) of proceeds from crime and financing of terrorism, shall submit the appropriate information to competent bodies of foreign states at their requests or by their own initiative in accordance with the procedure and on the grounds provided by international agreements of Russia. Transfer of information connected with revelation, withdrawal and confiscation of proceeds from crime to competent bodies of a foreign state shall be made, if it does not inflict damage on interests of national security of Russia, and can allow the competent bodies of this foreign state to commence investigation or state an inquiry. Information connected with revelation, withdrawal and confiscation of proceeds from crime shall be provided at the request of a competent body of a foreign state, provided it will not be used without preliminary consent of the appropriate state authorities of Russia which have provided it for purposes that are not stated in the inquiry. State authorities of Russia shall forward to competent bodies of foreign states inquiries on provision of the necessary information and give answers to requests made by these competent bodies in accordance with the procedure provided by the international agreements of Russia. State authorities of Russia performing activities connected with prevention of legalisation (laundering) of proceeds from crime and financing of terrorism, who forwarded a request shall

provide confidentiality of the supplied information and use it only for purposes stated in the request. In accordance with international agreements of Russia and federal laws, state authorities of Russia performing activities connected with prevention of legalisation (laundering) of proceeds from crime and financing of terrorism shall execute within their competence requests of competent bodies of foreign states on confiscation of proceeds from crime and financing of terrorism and on initiation of certain proceedings on revelation of proceeds from crime and financing of terrorism, imposition of arrest on property, on withdrawal of property, perform examinations, question the suspects, the accused, witnesses, victims and other persons, searches, withdrawals, transfer material evidence, impose arrest on property, hand over and dispatch documents. Costs connected with execution of the above requests shall be compensated in accordance with the international agreements of Russia.

Article 11. Recognition of the sentence (decision) of the court of a foreign state

In accordance with international agreements of Russia and federal laws, the Russian Federation recognises sentence (decision) made by courts of foreign states, which came into effect, with respect to persons having proceeds from crime. In accordance with international agreements of Russia, the Russian Federation recognises and executes sentence (decision) made by courts of foreign states, which came into effect, on confiscation of incomes drawn by criminal way, or property which is equal thereto, located on the territory of Russia. Confiscated incomes drawn by criminal way or property, which is equal thereto, may be transferred completely or partially to the foreign state whose court made the decision on confiscation on the basis of a specific international agreement.

Article 12. Delivery and transit transportation

Decision on the delivery to the foreign state of persons who committed crimes connected with legalisation (laundering) of proceeds from crime and financing of terrorism shall be made on the basis of obligations of Russia resulting from the international agreement of Russia. The same procedure shall be true for the decision on transit transportation of the above persons on the territory of Russia. If Russia does not have an appropriate agreement with the foreign state which asks for the delivery, these persons may be delivered for crimes connected with legalisation (laundering) of proceeds from crime and financing of terrorism subject to observance of the principle of reciprocity.

Chapter V. Conclusions

Article 13. Responsibility for infringement of this Federal law

Infringement by organisations performing operations with monetary funds or other assets and acting with the authority of a licence of requirements provided by articles 6 and 7 of this Federal law, except clause 3 of article 7 of this Federal law, may lead to withdrawal (annulment) of the licence in accordance with the procedure provided by the legislation of Russia. Persons guilty of infringement of this Federal law shall bear administrative, civil and criminal responsibility in accordance with the legislation of Russia.

Article 14. Public prosecutor's supervision

The General Prosecutor of Russia and public prosecutors subordinate shall perform supervision over execution of this Federal law thereto.

Article 15. Protesting against actions of the authorised body and its officials

An interested person shall have the right to apply to court for protection of his violated or contested rights and legal interests in accordance with the established procedure.

Article 16. Enforcement of this Federal law

This federal law shall come into effect from 1 February 2002.

Article 17. Bringing normative legal acts in line with this Federal law

Normative legal acts of the President of Russia and Government, laws and other normative legal acts of constituent entities of Russia shall be brought in line with this Federal law before its enforcement.

The President of the Russian Federation
V. Putin
Moscow, Kremlin
7 August 2001
No. 115-FZ

ANNEX 4: LAWS, REGULATIONS AND OTHER MATERIALS PROVIDED BY RUSSIA TO THE EVALUATION TEAM

PROVIDED WITH MUTUAL EVALUATION QUESTIONNAIRE

AML/CFT LAWS, REGULATIONS AND GUIDANCE

1. Decree 301rp on WG on AML Strategy
2. Decree 506rp on WG on AML Strategy
3. Law 115FZ AML CFT
4. MoF 132n Interagency Commission
5. Government 28 on Procedure for Registering Entities in Rosfinmonitoring
6. Government 173 on Procedure for NCCT List
7. Government 715 on Qualification Requirements for Compliance and Training
8. Government 840 on Model AML CFT Agreement
9. MoF 127n on Regulations of Territorial Body of Rosfinmonitoring
10. Rosfinmonitoring 149 on Regulations on Requests to Financial Organisations
11. Rosfinmonitoring 72 on Suspension of Operations
12. Rosfinmonitoring 104 Recommendations on Internal Control
13. Concept of National AML CFT Strategy
14. Government 245 on Regulations for Submitting Information by Organisations to Rosfinmonitoring
15. Government 425 on Submission of Information by State Bodies to Rosfinmonitoring
16. Government 1405r Model Agreement of Rosfinmonitoring
17. Rosfinmonitoring 86 Instructions on Submission of Information
18. Rosfinmonitoring 108 on Official Authorised to Draw Protocol on AO
19. Rosfinmonitoring 224 Qualifying Requirements for Rosfinmonitoring Staff
20. MoF 183n on Inspection of Rosfinmonitoring
21. Government 983R Recommendations on Internal Control
22. Government 307 FIU Regulations
23. Government 714 on Rosfinmonitoring staff
24. Government 186 FIU issues
25. Government 27 on Procedure for Listing Terrorists
26. Government 329 on Regulations on MoF
27. Government 6 on Approval of Internal Control Rules
28. MoF 88n on Regulations on Agreeing Internal Control Rules of Entities Without Supervisory Bodies
29. Rosfinmonitoring 164 on Registering Entities without Supervisory Bodies

INTERNATIONAL CONVENTIONS AND THEIR IMPLEMENTATION

30. Shanghai Convention on Combating Terrorism
31. Law 56FZ on Ratification CoE Convention Terrorism
32. Law 125FZ on Ratification CoE Convention on Corruption
33. Law 88FZ on Ratification International TF Convention
34. Law 114FZ Combating Extremist Activity
35. Law 121FZ on Ratification of European Convention Suppression of Terrorism
36. Law 127FZ on Ratification Protocol European Convention on Terrorism
37. Law 158FZ on Ratification Convention Nuclear Terrorism
38. Law 3FZ on Ratification Shanghai Convention
39. Law 26FZ on Ratification UN Palermo Convention
40. Law 40FZ on Ratification UN Convention against Corruption
41. Law 62FZ on Ratification Strasbourg Convention
42. Law 190FZ on Ratification Convention on Extradition
43. Law 1711-1 on Ratification UN Vienna Convention
44. Decree 6 on UNSCR 1373
45. Decree 116 on Combating Terrorism
46. Decree 786 on UNSCR 1267

FINANCIAL - BANKING

47. BoR Instructions 109 I on Registering and Licensing Banks
48. Law 40FZ on Bankruptcy
49. Law 86FZ on BoR
50. Law 395-1 on Banks and Banking Activity
51. BoR 12T 2003 on Control over Correspondent Relations
52. BoR 99T Recommendations on Internal Control
53. BoR and Taxation Ministry on Procedure for Registration of Credit Institutions
54. BoR Directive 1317U on Correspondent Relations with Offshore
55. BoR Directive 1485U on Training Requirements
56. BoR Directive 1486U on Qualifying Requirements
57. BoR Instruction 76I on Regulating Banks with Branches Abroad
58. BoR letter 15T on Relations with Montenegro
59. BoR Letter 92T on Managing Legal Risk
60. BoR Letter 100T on FATF Typologies Report
61. BoR Letter 171T on Nauru
62. BoR Regulation 207P on Submission of Information
63. BoR Regulations 242P on Internal Control
64. BoR Regulations 264 on Revocation of Licenses
65. BoR Regulations 271P on Decisions on Registering and Licensing Banks
66. Law 177FZ on Insuring Deposits in Banks
67. Government and BoR on Strategy of Development of Banking Sector

68. BoR Regulation 2P on Non Cash Settlements
69. BoR 12T on Supplying State Register Info to Banks
70. BoR 17T on Control over Cash Operation for AML CFT
71. BoR 97T on Suspension Operations for as CFT in Banks
72. BoR 222P on Non Cash Settlements by Individuals
73. BoR 28I on Opening BoR Accounts
74. BoR 103-T on Control over Implementation of AML CFT Law
75. BoR 1519U on Sending Info on Refusals in Operations
76. BoR 24T on Wolfsberg Principles
77. BoR 115T on AML and Internet Banking
78. BoR 161T on Preventing Doubtful Operations
79. BoR Regulation 262P on Identification of Clients
80. BoR 479 Recommendations on AML Work

FINANCIAL – SECURITIES

81. Law 39FZ on Securities Market
82. FSFM 05-16 PZN on procedure for Inspections
83. FSFM 613r Recommendations for Securities Market Participants
84. Law 156FZ on Investment Funds
85. FSFM 06-29 PZN on Internal Control in Securities Professional participants
86. Government 317 Regulation on FSFM

FINANCIAL - SECURITIES

87. Law 39FZ on Securities Market
88. FSFM 613r Recommendations for Securities Market Participants
89. Law 156FZ on Investment Funds
90. FSFM 06 29 PZN on Internal Control in Securities Professional participants
91. Government 317 Regulation on FSFM

FINANCIAL - INSURANCE / PENSION FUNDS

92. Law 75FZ on Non State Pension Funds
93. Law 4015 1 on Insurance Activity
94. Government 330 on Regulations for Insurance Supervision Service
95. Government 203 on Federal Insurance Supervision Service
96. Government 432 on Licensing Certain Activity in Financial Markets

FINANCIAL - FOREX

97. BoR 12T 2005 Recommendations on Control over Purchase Securities and Currency
98. BoR Instructions 113 I on Exchange Offices
99. Law 173FZ on Currency Regulation and Control

DNFBPs - LAWYERS, NOTARIES AND ACCOUNTANTS

100. Law 63FZ on Lawyers
101. Law 4462 1 on Notariate
102. Government 82 on Reporting by Lawyers Notaries Accountants

DNFBPs - DEALERS IN PRECIOUS METALS AND STONES

103. Law 41FZ on Precious Metals and Stones
104. Decree 742 on Export of Precious Stones
105. Government 64 on Handling Precious Stones
106. Government 64 on Organisations Controlling Extraction of Precious Stones
107. MoF 76n on Regulations of Assay Control in Precious Metals Stones
108. MoF 77n on Regulations on Agreeing Internal Control Rules for Precious Metals
109. Customs 1386 on Instruction for Custody for Currency and Jewellery
110. MoF 91 Regulations on State Assay Chamber
111. Assay Chamber 47 Recommendations on Internal Control

DNFBPs - TCSPs / TRUSTS / COMPANY LAW / SPECIAL ECONOMIC ZONES

112. Law 14FZ on Limited Liability Companies
113. Law 128FZ on Licensing Specific Types of Activity
114. Law 129FZ on State Registration of Entities
115. Law 116FZ on Special Economic Zones
116. Law 208FZ on Joint Stock Companies

DNFBPs - GAMING

117. Law 138FZ on Lotteries
118. Law 244FZ on Regulation of Gaming Activity
119. Government 793 on Authorised Body in Gambling

CUSTOMS

120. Customs Code
121. Law 114FZ on Exit and Entry into Russia
122. Decree 468 on Export Control Commission
123. Law 114FZ on Service in Customs Bodies
124. Law 4730 1 on State Border
125. Government 718 on Customs Duties for Goods Brought by Persons
126. Government 459 Regulation on Customs Service

LEGAL AND LAW ENFORCEMENT

127. Civil Procedure Code
128. Code on Administrative Offences
129. Criminal Code
130. Decree 927 Regulations on the Ministry of Internal Affairs
131. Decree 960 Regulations of Federal Security Service
132. Decree 976 Regulations on Drug Control Service
133. Law 40FZ on Federal Security Service
134. Law 2202-1 on Prosecution Office
135. Supreme Court Plenum Decision 23 on ML
136. Government 925 on Federal Property Fund
137. Civil Code Part One
138. Code of Criminal Procedure
139. Government 653 on Model Agreement of the Ministry of Internal Affairs with Foreign Counterparts
140. Law 144FZ on Operational Search Activity
141. Law 35FZ on Combating Terrorism
142. Prosecution 26 on Strengthening Prosecution AML Supervision

NPOs

143. Law 7FZ on Non Profit Organisations

144. Law 82FZ on Public Associations

OTHER

145. Constitution of Russia
146. Decree 314 on System of Executive Structure
147. Decree 1300 on National Security Concept
148. Labour Code
149. Law 62FZ on Citizenship
150. Law 101FZ on International Treaties
151. Law 115FZ on Legal Status of Foreigners
152. Law 126FZ on Communications
153. Law 176FZ on Postal Communications
154. Decree 129 on Working Group on Corruption
155. Decree 320 on Federal Service in Communications Supervision
156. Decree 484 on Submission of Information on Income by Civil Officials
157. Decree 649 on Structure of Executive Bodies
158. Government 199 on Taking Decision on Undesirability of Entrance of Foreigners
159. Government 362 on Commission on Combating Drugs
160. Government 1449r on Participation in EAG
161. Government 1696r on Participation in FATF
162. Government 1989r on EAG Training Centre
163. Law 58FZ on System of State Service
164. Law 134FZ on Protection of Entities in Supervision
165. Law 135FZ on Protection of Competition
166. Law 281FZ on Special Economic Measures
167. Government 110 on Procedure for Supervision in Communications
168. Law 79FZ on State Civil Service
169. Decree 601
170. Decree 1263 on Establishing FMC
171. Law 82FZ on Minimum Wage
172. Law 164FZ on Financial Leasing

PROVIDED AT A LATER STAGE

173. Agreement on Co-operation Between Rosfinmonitoring and the Federal Chamber of Notaries (12 July 2007)
174. Agreement on Co-operation Between Rosfinmonitoring and the Federal Chamber of Lawyers (12 July 2007)
175. BoR of Russia Letter No. 7-T of 20 January 2003 on Implementation of AML/CFT Law
176. BoR of Russia Instructions No. 105-I of 25 August 2003 on Conducting Inspections of Banks
177. BoR Directive No. 179-T of 24 Dec 2003 on Funds Transfers (Non-Account Holders) and Transactions using Pre-paid Financial Products
178. BoR of Russia Letter No. 99-T of 30 June 2003 on Release of Data Covered by Banking Secrecy
179. Civil Code of the Russian Federation: Article 857 – Banking Secrecy
180. Civil Code of Russia: Chapter 58. 'Gaming and Betting' (Articles 1062-1063)
181. Federal Law No. 117-FZ of 23 June 1999 on Protection of Competition in the Financial Services Market
182. Tax Code of Russia: Chapter 29. 'Gambling Business Tax'
183. Interagency agreements of the FCS
184. Customs declaration forms
185. Annex to order 290 of Russia Post
186. Annex to regulation 285 of Russia Post
187. Order 10 of 12.01.04 by Russia Post
188. Order 290 by Russia Post
189. Russia Post regulation
190. BoR of Russia letter 8
191. BoR of Russia letter 9
192. Government 173 on Procedure for NCCT List English
193. Order of FMC No.18
194. Order of FMC No.18 amended
195. Order of FMC No.7
196. Order of Rosfinmonitoring No. 13
197. Order of Rosfinmonitoring No. 53
198. Agreements by Federal Tax Service
199. Lawyers Code
200. Notary Code
201. Act BoR of Russia
202. Act Rosfinmonitoring
203. Act Rosstrahnadzor
204. Act Rossviaznadzor
205. Act on Rec. 19 (AML/CFT Law amendment)
206. Explanatory Note for Act on Rec. 19
207. Code of Criminal Procedure w/changes
208. Regulations on Investigative Committee of Prosecution Office
209. Government decision on incentives 611
210. Draft law on PEPs and SR VII (English)
211. BoR Letter on Amanbank, Kyrgyzstan
212. BoR Letter on Asianunversalbank, Kyrgyzstan
213. Rosfinmonitoring Annual Report 2006
214. Federal Law 115FZ amended
215. Information sharing agreement Rosfin and Customs FAR EAST FEDERAL DISTRICT
216. Information sharing agreement Rosfin and Customs
217. Rosfinmonitoring powers and duties amended
218. Supreme court decision
219. FTS letter on mass-registration addresses No. 09-1-03/3103 of June 16, 2006
220. FTS Order P-312
221. BOR Decision 6
222. BoR Letter 170-T of October 30, 2007 on enhanced due diligence for foreigners
223. BoR Letter No. 8-T of January 18, 2008 on definition of PEPs
224. MoF Decision 109N OF DECEMBER 11, 2001 on new technologies in the securities sector
225. BoR Letter 44-T dated April 5, 2007 on supervision over remote banking operations
226. BoR Letter 60-T dated April 27, 2007 on EDD in remote banking operations
227. Law 152-FZ dated July 27, 2006 on personal data
228. Accounting Law 129-FZ
229. Instruction 105-1

230. MoF order 108N amended February 4, 2004 on internal accounting of operations in securities market
231. BOR regulation 2-P(amended)
232. BOR regulation 222-P(amended)
233. BOR letter 12-T
234. BOR Letter 15-T
235. Russia Post Order 507 on internal control rules (03 November 2005)
236. Russia Post Order 459 on internal control rules (18 September 2007)
237. BoR Regulation 290-P, July 4, 2006 on foreign activities of subsidiaries
238. BoR Instructions 130-I, February 21, 2007 on purchase of shares in banks
239. BOR instruction 109-1
240. Law 134-FZ on supervision
241. Government decision 110
242. BoR letter 98-T, July 13, 2005 on sanctions for AML/CFT breaches
243. BoR directive 1842-U, June 20, 2007 on payment acceptance and transfers
244. Law 119-FZ on auditing
245. Rosfinmonitoring risk based supervision methodology
246. Law 172-FZ on amendments to Insurance law
247. Law 177-FZ on insurance of deposits
248. Law 181-FZ on amendments to Banking law
249. Rosarchive list on record keeping
250. Ethics Code of auditors
251. FTS Order NO. SAE-3-09/325, JULY 15, 2005 on supply of registry information to CIs
252. Government decision 6, January 8, 2003 on approval of internal control rules
253. Rosfinmonitoring supervisory methodology
254. Government Decision 743 of November 3, 2007 on amendments to Decisions 983R and 28
255. MoF Letter December 19, 2006 № 07-05-
256. Government decision on ROSCOM 354, June 6, 2007
257. FSFM Order NO. 07-108/PZ-N OF NOVEMBER 13, 2007 on supervision procedures
258. MoF letter NO. 07-03-01/647 of JUNE 27, 2005 on AML/CFT regulation of accountants
259. AML/CFT recommendations to lawyers

ANNEX 5: PREDICATE OFFENCES COVERED BY ARTICLES 174, 174.1 AND 175 CRIMINAL CODE

FATF designated category of offences	Predicate offences stipulated in the Criminal Code	Does the predicate offence apply to the three money laundering offences 174, 174.1 and 175?
Participation in an organised criminal group and racketeering	• 163 Extortion • 210 (criminal organisation) • 209 (banditism)	Yes
Terrorism, including terrorist financing	• 205 (terrorism) • 205.1 (financing of terrorism)	Yes. However, as noted in section 1.2 of this report, the criminalisation of terrorist financing is not sufficient.
Trafficking in human beings and migrant smuggling	• 127.1 (human being trafficking) • 322.1 (organising illegal migration)	Yes
Sexual exploitation, including sexual exploitation of children	• 240 (forcing prostitution) • 241 (organising prostitution)	Yes
Illicit trafficking in narcotic drugs and psychotropic substances	• 188 (smuggling, incl smuggling of psychotropic substances) • 228 (being and selling of contraband, including psychotropic substances) • 228.1 (producing narcotics) • 229 (stealing or extortion of narcotics)	Yes
Illicit arms trafficking	• 189 (illegal export of WMD and other military hardware) • 222 (illegal handling of firearms)	Yes
Illicit trafficking in stolen and other goods	• 175 (fencing / receiving stolen goods)	Yes
Corruption and bribery	• 201 - 202 (abuse of authority) • 204 (commercial bribery) • 290 - 291 (bribery)	Yes
Fraud	• 159 (fraud)	Yes
Counterfeiting currency	• 186 – 187 (counterfeit banknotes, securities debit cards, credit cards and other payment documents)	Yes
Counterfeiting and piracy of products	• 146 – 147 (violation of copyrights and patents) • 180 (illegal use of a trademark)	Yes, but limited
Environmental crime	• 246 – 262 (ecological crimes)	Yes
Murder, grievous bodily injury	• 105 (murder) • 111 (grave injury)	Yes
Kidnapping, illegal restraint and hostage-	• 126 (abduction) • 127 (illegal deprivation of liberty)	Yes

FATF designated category of offences	Predicate offences stipulated in the Criminal Code	Does the predicate offence apply to the three money laundering offences 174, 174.1 and 175?
taking	• 206 (hostage taking)	
Robbery or theft	• 158 (theft) • 161 – 162 (robbery)	Yes
Smuggling	• 188 (smuggling)	Yes
Extortion	• 163 (extortion)	Yes
Forgery	• 171 (official forgery) • 233 (forgery of prescriptions to receive narcotics) • 327 (forgery of official documents)	Yes, but limited
Piracy	• 227 (piracy)	Yes
Insider trading and market manipulation.	• Not covered	No