INTERNATIONAL MONETARY FUND

RUSSIAN FEDERATION

FINANCIAL SECTOR ASSESSMENT PROGRAM

September 2016

TECHNICAL NOTE

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT)

Prepared By

Legal Department

This Technical Note was prepared by IMF staff in the context of the Financial Sector Assessment Program (FSAP) mission in the Russian Federation, led by Karl Habermeier and overseen by the Monetary and Capital Markets Department. It contains technical analysis and detailed information underpinning the FSAP's findings and recommendations. Further information on the FSAP can be found at http://www.imf.org/external/np/fsap/fssa.aspx.

CONTENTS

Glossary

AML	Anti-money laundering
BO	Beneficial ownership
CBR	Central Bank of Russia
CDD	Customer due diligence
CFC	Controlled foreign company
CFT	Combating the financing of terrorism
CRA	Center of Risk Assessment of ML/TF
CTR	Cash transaction reports
DNFBP	Designated Non-Financial Businesses and Professions
EAG	Eurasian Group on Combatting Money Laundering and Financing of Terrorism
FATF	Financial Action Task Force
FI	Financial Institutions
FSAP	Financial Sector Assessment Program
FTS	Federal Tax Service
LEA	Law enforcement authority
MER	Mutual Evaluation Report
ML	Money laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
NRA	National Risk Assessment
OSCE	Organization for Security and Co-operation in Europe
PEP	Politically Exposed Person
RF	Russian Federation
ROSC	Report on the Observance of Standards and Codes
Rosfinmonitoring	Federal Financial Monitoring Service
STR	Suspicious transaction report
TN	Technical note
TF	Terrorist Financing
USRLE	Unified State Register of Legal Entities

EXECUTIVE SUMMARY[1]

This technical note (TN) sets out the findings and recommendations made in the Financial Sector Assessment Program (FSAP) for the Russian Federation (RF) in the areas of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT). It summarizes the findings of a targeted review of several aspects of the RF's progress in addressing vulnerabilities in the financial sector, specifically the banking sector. A full assessment of the AML/CFT framework against the current FATF standard will be conducted by the FATF, Eurasia Group and MONEVYAL, and will be available in 2019. Although significant steps have been taken to strengthen the AML/CFT regime since the 2008 mutual evaluation report, the authorities are continuing to bring the AML/CFT framework in line with the 2012 FATF standard and improving its effectiveness.

Some authorities have improved their understanding of money laundering and terrorist financing (ML/TF) risks, however the swift finalization of the national risk assessment (NRA) will further advance that understanding and the use of risk-based approach by all concerned agencies and reporting entities. Some concerned authorities are cognizant of the main threats (e.g., fraud, corruption, TF) and vulnerabilities (e.g., one-day firms). The current understanding of ML/TF risks may, however, be limited because it mostly relies only on analysis from Rosfinmonitoring and Central Bank of reports and data provided mostly by the banking sector. This limitation could understate the magnitude of criminal proceeds in other sectors (e.g., real estate, lawyers, and precious metals and stones). The RF authorities have initiated the NRA process that will involve a broad spectrum of stakeholders and lead to the development of a national strategy for prioritizing AML/CFT policies and activities.

The authorities took measures to prevent the abuse of Russian companies for ML/TF purposes, but more efforts are needed to ensure that timely and accurate beneficial ownership information is available to the authorities. The strengthened legal requirements on information on beneficial owners and the new law for identifying Russian tax residents who are beneficial owners of foreign companies (de-offshorization) are positive developments. Although the beneficial ownership (BO) information is accessed, when available, and shared in a timely manner, the authorities should continue improving its availability and accuracy.

Preventive measures related to politically exposed persons (PEPs) and reporting of suspicious transactions were updated and are largely in line with the FATF standards, however the PEPs definition requires further amendments and the effectiveness of the measures should be enhanced further. Addressing the gaps in the definition of PEPs could enhance the effectiveness of banks in addressing the risks of laundering the proceeds of corruption. The suspicious transaction reporting system generates a significant quantity of reports, but there is a need to improve the quality of reporting in view of the country's ML/TF risk profile.

[1] This note was prepared by Chady El-Khoury and Jonathan Pampolina (IMF's Legal Department).

The AML/CFT supervision of banks is comprehensive and related sanctions are effective, but further progress could be made to enhance risk-based supervision and AML/CFT tools. The existing risk-based supervisory methodology appears limited as it relies on a checklist of predetermined criteria rather than a robust analysis of indicators of ML/TF risks. Comprehensive data on the nature and potential exposure to ML/TF risks at the institutional level could improve the implementation of risk-based supervisory tools. Sanctions, particularly the revocation of bank licenses, owing to AML/CFT violations have ramped up in recent years, and are considered effective and dissuasive leading to improving of compliance of banks.

Table 1. Main FSAP Recommendations for AML/CFT

Recommendations	Priority
Assessing and Understanding ML/TF Risks	
i. To complete and share the results of national assessment of ML/TF risks with the stakeholders.	Near
ii. To prepare a national AML/CFT strategy that would prioritize AML/CFT policies and activities and allow the use of risk based approach by concerned authorities	Intermediate
Entity Transparency and availability of beneficial ownership information	
i. To improve the availability and accuracy of BO information (through the customer due diligence of banks, the creation of a register for BO information or requiring companies to have relevant BO information at the premises level) and ensure robust implementation of sanctions against persons who do not comply with the information requirements	Near
Preventive Measures	
i. To ensure that the definition of PEPs fully aligns with the FATF standards to include all categories of prominent public officials, family members, associates including when PEPs are beneficial owners	Near
ii. To provide guidance to banks in identifying and accepting, and managing business relations with customers who are PEPs, including for domestic PEPs, their family members and associates	Intermediate
iii. Provide guidance on typologies and timely feedback to banks on quality of suspicious transactions reports to align the reporting with the ML/TF risks in Russia	Near
Supervision	
i. To improve the CBR's identification and understanding of ML/TF risks and controls, and develop further the risk-based approach tools for offsite and onsite supervision (with a focus on PEP and BO-related requirements).	Near
ii. To ensure effective implementation of a broad range of sanctions against financial institutions that are dissuasive and proportionate to the severity of the AML/CFT violations.	Intermediate

INTRODUCTION

1. This Technical Note (TN) provides a targeted review of the Russian Federation's AML/CFT system in the context of the Financial Sector Assessment Program (FSAP).[2] It does not constitute an assessment or evaluation of the RF's AML/CFT system. A full assessment against the current FATF standard will be available in 2019.

2. As discussed with authorities prior to the beginning of this exercise, staff's review focuses mainly on the RF's efforts to address certain vulnerabilities in the banking sector related to the availability of beneficial ownership information, transparency of companies, preventive measures relating to PEPs, suspicious transaction reporting, and risk-based AML/CFT supervision. These represent key shortcomings identified in the 2008 mutual evaluation report (MER)[3] of the RF, which may have had a significant impact on the effectiveness of the country's AML/CFT regime.

3. Staff analysis is based on a range of materials and benefitted from discussions with authorities. Staff reviewed available information including the most recent MER from 2008, the documentation submitted by the RF to FATF and MONEYVAL on progress made since the last mutual evaluation. The analysis also draws on the authorities' responses to questions submitted by staff ahead of the FSAP, and discussions held during the mission undertaken from February 1–5, 2016, when staff met with officials of the Central Bank of Russia (CBR), the Federal Financial Monitoring Service (Rosfinmonitoring)- Russia's Financial Intelligence Unit, the Ministry of Internal Affairs, the Prosecutor General's Office, the Federal Taxation Service, the Federal Security Service, and representatives of two banks.

PROGRESS SINCE THE LAST ASSESSMENT

4. In the 2008 MER, assessors found a number of shortcomings in the RF's AML/CFT framework. The 2008 MER identified key deficiencies in the framework, including, among others, the lack of adequate transparency of information on the beneficial ownership and control of legal

[2] Under current FSAP policy, every FSAP should incorporate timely and accurate input on AML/CFT. Where possible, this input should be based on a comprehensive AML/CFT assessment conducted against the prevailing standard. In instances where a comprehensive assessment against the prevailing standard is not available at the time of the FSAP, as is the case with the U.S., staff may derive key findings on the basis of other sources of information, including already available information or information obtained in the context of the FSAP. See the Acting Chair's Summing Up—Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism—Executive Board Meeting 14/22, March 12, 2014, BUFF/14/23.

[3] The RF's AML/CFT system was last assessed, and the MER adopted and published in 2008—see http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Russia%20ful.pdf. The assessment was conducted jointly by the FATF, the Eurasian Group and the MONEYVAL Committee of the Council of Europe (MONEYVAL) against the 2003 FATF 40+9 Recommendations and on the basis of the corresponding assessment methodology. The RF is expected to undergo a comprehensive assessment against the FATF's revised standard and methodology in 2019. An onsite mission is planned for November/December 2018, with plenary consideration of the draft mutual evaluation report scheduled for June 2019.

persons established in the RF, and insufficient guidance to banks on dealing with customers who are foreign PEPs. Accordingly, the FATF placed the RF under its regular follow-up process and called on authorities to address these gaps.

5. Since 2008, the Russian authorities have taken significant steps to strengthen the country's AML/CFT regime. They have strengthened the AML/CFT law to address the identified gaps, including by aligning the definition of "beneficial owner" with the FATF standard and introducing a prohibition against individuals with criminal convictions from acquiring or controlling a significant amount of shares in certain credit institutions.[4] In addition, the CBR issued guidelines for the implementation of enhanced customer due diligence measures for foreign PEPs, and extended the requirements for domestic PEPs. Owing to progress made, the RF subsequently exited the FATF's follow-up process in 2013.[5]

6. The RF has yet to be assessed against the prevailing FATF standard. The FATF standard and methodology were revised in 2012 and 2013, respectively, placing a greater emphasis on a risk-based approach to AML/CFT and on assessing the effectiveness of AML/CFT regimes. Specifically, the revised standard now highlights the need for countries to identify, assess and understand their ML/TF risks, and extends enhanced customer due diligence obligations beyond foreign PEPs to cover domestic PEPs. The FATF, EAG, and MONEYVAL are scheduled to jointly assess the RF's AML/CFT regime under the prevailing standard in late 2018.

ASSESSING AND UNDERSTANDING RISK

A. Context and Risk

7. The main ML/TF risks discussed during the 2008 assessment were related to the abuse of shell companies. In the 2008 MER, the assessors concluded that the Russian authorities were aware of the ML/TF schemes generally used in the country. At that time, many ML schemes were said to have involved the misuse of legal entities and financial institutions (FIs), but the overwhelming majority were associated with "one-day" firms.[6] Bank accounts and financial instruments were used in the layering stage of the money laundering schemes, where a large number of bank accounts are opened in the names of different persons, commercial organizations or front companies.

8. Rosfinmonitoring currently assesses the ML/TF threats by relying on the analysis of suspicious transaction reports (STRs), cash transaction reports (CTRs) and other information it receives and collects. The President of the RF tasked the agency with developing strategies and measures to counter the identified ML/TF threats.[7] The agency is well-placed to coordinate efforts

[4] Specifically, see Federal Law No. 134-FZ (June 28, 2013) and Federal Law No. 146-FZ (July 2, 2013).

[5] FATF, Russian Federation: 6th Follow-Up Report (October 2013).

[6] These are commercial organizations registered under the names of non-existent persons without intention to perform any real commercial activity. (2008 MER, page 13).

[7] Presidential Decree No. 808, dated June 13, 2012.

considering the large amounts of information it receives from STRs, threshold reports filed by FIs, its access to information and databases of other state bodies,[8] and cooperation with government agencies and the private sector. Within Rosfinmonitoring, a Center of Risk Assessment of ML/TF (CRA) was established to regularly identify the areas of ML/TF risks through, operational and strategic analysis. The CRA reports annually its confidential findings to the President.

9. Based on the analysis of STRs and additional data received and collected, Rosfinmonitoring has identified some ML/TF threats facing the country. In terms of money laundering, there is a broadly shared view among the authorities that the main threats come from fraud and corruption. Fraud (e.g., account fraud, fraudulent loans, and identity fraud) was found to be the most common predicate crimes detected by authorities. Corruption is a key concern from a threat perspective[9], due to the perceived level of proceeds generated by the activity.[10] Corruption in the defense industry and construction, among others, was an issue highlighted by the Rosfinmonitoring's CRA annual report. Nevertheless, Russia has made some progress in tackling corruption, having improved its ranking in Transparency International's Corruption Perception Index to 119 (out of 168 countries) in 2015 from 136 (out of 174 countries) in 2014.[11] In addition, Presidential Decree No. 147 (April 1, 2016) set up an anti-corruption plan focusing on exposing corruption including by improving the beneficial ownership information, driving out the culture of corruption, and enhancing international cooperation.[12] As regards terrorist financing, the authorities cited the activities of armed gangs in the North Caucasus, the operations of cells of international terrorist organizations in the country's territory, and Russian citizens travelling to conflict areas to join international terrorist organizations (e.g., Islamic State of Iraq and Levant) as the main TF threats.

10. The authorities are also cognizant of the main vulnerabilities in the system. Shell companies ("one-day" firms) present a particular vulnerability, which is prone to abuse for ML purposes. One-day firms are legal entities that are set up without any intention of ever performing real commercial activity, but with the goal of acting as a formal party in a financial transaction, often to pursue unlawful purposes.[13] The ability of one-day firms to perform illegal financial operations

[8] E.g., Federal Tax Service, Ministry of Internal Affairs, Ministry of Finance, Rosfinnadzor, Federal Treasury, Prosecutor's General Office, Investigation Committee, Federal Drug Control Service, Federal Customs Service, Federal Security Service, the CBR, Rosstat, Russian Assay Office, etc.

[9] President Putin, in his first state-of-the-union speech since returning to the presidency—December 2012, focused largely on domestic issues, saying that fighting corruption is one of the key priorities of his third presidential term and that Russia should look for guidance in its own history.

[10] See European Parliamentary Research Service, Corruption in Russia (2014). (Available via the Internet: http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140742/LDM_BRI(2014)140742_REV1_EN.pdf)

[11] Transparency International, Corruption Perceptions Index 2015. (Available via the Internet: http://www.transparency.org/cpi2015/#results-table)

[12] Russian Federation, Country Statement in the UK Anti-Corruption Summit, London (2016). (Available via the Internet: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/522727/Russian_Federation.pdf)

[13] OECD, Global Form on Transparency and Exchange of Information for Tax Purposes Peer Reviews: Russian Federation (2014).

(including the movement of illicit proceeds of crime) indeed presents significant ML risks, as more than two trillion roubles of financial transactions (volume) were reportedly carried out by these shell companies in 2015, according to authorities. The authorities have also identified current technologies (e.g., wire transfers and crowdfunding) as vulnerabilities that could be exploited for TF activities. Terrorists and their accomplices are said to actively use modern technologies (e.g., e-payment systems, mobile banking), which afford them anonymity in sending minor amounts through the Internet and other social networks. Crowdfunding (the mass collection of voluntary donations of funds or other assets from different individuals) likewise provide mobile and quick fund collection activities that terrorists and terrorist organizations can take advantage of in raising funds.

11. The revised FATF standard now calls on countries to identify, assess, and understand their ML/TF risks. It looks at how national AML/CFT policies and strategies address the identified ML/TF risks, which goes beyond being cognizant of prevailing ML/TF schemes and typologies.

12. The RF authorities have therefore initiated the NRA that is expected to be completed early 2017. The President recently approved amendments to the Rosfinmonitoring's regulations, which authorizes the agency to organize a NRA.[14] The exercise foresees the involvement of the CBR, relevant federal executive bodies, and other state bodies and organizations, with the participation of representatives of the financial sector. The authorities will rely on the FATF guidelines on data and statistics as well as inputs from MONEYVAL and the OSCE. Under the proposed amendment, a public sanitized version of the results of the NRA will be published on the Rosfinmonitoring's website.

13. Although the authorities do not have a national AML/CFT strategy, they provided information about the extent to which related national policies and activities address the main ML/TF risks in Russia. In particular, some legislative measures to address the identified threats and vulnerabilities have been introduced, while others are being considered. Several laws were recently enacted: (a) to require enhanced customer identification in respect of new technologies (e.g., transfers between individuals and cross-border money transfers);[15] (b) to oblige FIs to conduct customer identification of foreign entities that do not have legal personality in the country (e.g., trusts, foundations, and partnerships);[16] (c) and to strengthen information exchange between the CBR and Rosfinmonitoring on customers of FIs, who are involved in ML/TF.[17] A draft law requiring legal entities to identify and document their beneficial owners and providing penalties for violation has also been submitted to parliament. In addition to creating an interdepartmental commission on combatting TF, work is being carried out to strengthen the criminal penalties for involvement in terrorist activities, including the acts of aiding and abetting. The authorities have also engaged with the private sector to raise awareness on some identified ML/TF risks. However, the authorities have not considered adopting a comprehensive strategy(ies) or policy(ies) to address these risks and enhance the effectiveness of the framework through better use of resources. They may nevertheless

[14] Presidential Decree No. 103, dated March 8, 2016.

[15] Federal Law No. 110-FZ (May 5, 2014).

[16] Federal Law No. 424-FZ (December 30, 2015).

[17] Federal Law No. 424-FZ (December 30, 2015).

do so after completing the NRA. Additionally, the measures taken by the authorities are focused both on the legal framework and to some extent on improving the effectiveness of the regime. Overall, the authorities demonstrated different levels of understanding of the ML and TF risks, across the threats, transnational aspects, and vulnerabilities.

14. The authorities' understanding of ML threats (stemming from the domestic criminal environment) relies heavily on Rosfinmonitoring's analysis of STRs and CTRs provided mostly by the banking sector and may understate the magnitude and potentially ignore critical contributing crimes such as tax evasion,[18] corruption, and fraud in other sectors (e.g. real estate, nonbank FIs). In terms of transnational ML activity, they also demonstrated some understanding of the destinations used for laundering and showed a common understanding of how the proceeds are moved in and out Russia through the banking sector. However, their understanding about the volume of such proceeds and laundering through other channels was less developed. The authorities presented conflicting assessments about the main assets used for ML in Russia. Some saw Russian ML activity as mainly cash or "near cash" based, while others understood that such activities also involved the purchase of nonfinancial assets (such as real property or other high value goods). Overall, the understanding of risks related to the financial sector was higher than risks related to DNFBPs.

B. Conclusions and Recommendations

15. The authorities are making efforts aimed at identifying, assessing, understanding and mitigating the RF's ML/TF risks, but further action is needed to finalize and communicate the results of the NRA. The authorities should proceed with the planned assessment of national ML/TF risks, prior to the scheduled FATF/EAG/MONEYVAL assessment in 2018. The authorities should use an inclusive and multi-faceted approach to assessing the ML/TF risks. They should rely on qualitative and quantitative information (beyond the analysis of STRs and CTRs) provided by all concerned agencies, reporting entities including designated non-financial businesses and professions, and academics. A sanitized version of the main results of the NRA should be shared with all concerned agencies and the private sector. Based on the results of the NRA, it is recommended that authorities also adopt and communicate a national AML/CFT strategy and propose prioritized action items to address and mitigate the identified ML/TF risks. This approach should be an essential foundation to efficient allocation of resources across the AML/CFT regime and the implementation of risk-based measures through the framework.

[18] The revised FATF standard requires that countries provide in their domestic law that tax crimes are predicate offenses to ML. While the standard does not contain a definition of "tax crimes," it requires that countries apply the crime of ML to all serious proceeds-generating offenses.

TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS IN RUSSIA

A. Background and Risk

16. There are several types of legal entities in the RF. These include the following commercial entities: general partnerships, limited partnerships, limited liability companies, double liability companies, joint stock companies, production co-operatives, and unitary enterprises. Information on the creation and types of legal persons that may be established under Russian law is available online through the Federal Tax Service (FTS) website. Basic information is also accessible through online consultation. As of end-2015, 4,820,432 legal entities were registered in Russia, most of which were limited liability companies.[19] All of them are required to provide to the Unified State Register of Legal Entities (USRLE) basic information on the commercial entity, such as legal form, information on founders, the identity of persons entitled to act on behalf of the legal entity, taxpayer identification number and information on bank accounts of the legal entity.[20] At the time of the 2008 MER, commercial entities were not required to retain beneficial ownership information, nor were they required to register such information in the USRLE. In addition, there was no explicit requirement for FIs or designated non-financial businesses and professions (DNFBPs) to identify beneficial owners of legal persons.

17. Access to ownership information is particularly relevant in the context of the authorities' difficulties in addressing the ML risks associated with "one-day" or shell companies. As identified by the authorities, shell companies pose a high risk and are often used as a front to open bank accounts without revealing the identity of the beneficial owner(s). In addition, corporate vehicles are a common method used to veil the identity of the beneficial owner(s) and place, layer, and integrate illicit proceeds in the financial system.

B. Availability of the Beneficial Ownership Information

18. The authorities have strengthened the legal requirements on ownership information since the 2008 MER. A 2013 amendment to the AML/CFT law[21] added a definition of beneficial owner that is consistent with the FATF standard.[22] It also required FIs and DNFBPs to take measures to identify and verify the beneficial owner.

[19] The number includes (a) 3,962,627 limited liability companies; (b) 126,074 joint stock companies; (c) 21,650 production co-operatives; and (d) 23,262 unitary enterprises.

[20] Federal Law No. 129-FZ, August 8, 2001.

[21] Federal Law No. 134-FZ, June 28, 2013.

[22] "Beneficial owner means for the purposes of this Federal Law a natural person who directly or indirectly (through third persons) owns (has a predominant stake of over 25 percent in the capital of) a client being a legal entity or has the possibility of controlling the actions of the customer." (Federal Law No. 115-FZ, as amended).

19. The amended framework on identification and verification of beneficial owners is broadly in line with the revised FATF standard. Under the revised FATF standards, where no natural person is identified as the beneficial owner of a legal person, FIs should identify and take reasonable measures to verify the identity of the relevant natural persons who holds the position of senior managing official.[23] Although FIs are not explicitly prohibited from establishing or continuing a business relationship with customers in cases where the customer's beneficial owner cannot be identified, or his/her identity cannot be verified[24], they are nevertheless prohibited from opening an account when the customer refuses to provide BO information and have the right to refuse to carry out the customer's transactions, and to terminate the contract[25] in cases where the customer fails to provide relevant information. The RF's AML/CFT law provides that in cases of a failure to identify the beneficial owner, the FI may recognize the sole executive body (position of senior managing official) of the customer as the beneficial owner.[26] In implementation, banks might often have recourse to designating the senior manager as BO, and therefore the law and related implemented regulations might clarify that such measure should only be used as a last resort.

20. The "de-offshorization"[27] law provides a new framework for determining the identity of Russian tax residents, who are beneficial owners of foreign companies.[28] It provides for the determination of a controlled foreign company (CFC), which is a foreign company that is not a Russian tax resident, but is nevertheless controlled by a Russian tax resident. Among other things, a Russian tax resident is deemed to be a controlling person of a CFC and fall within the ambit of the law, if his/her participation or interest in the CFC is at least 50 percent during 2015 and 25 percent thereafter. Profits received by a Russian tax resident from a CFC will thus be subject to taxes with specific qualifications (e.g., double tax agreements). The authorities claim that information on CFCs controlled by Russian tax residents can be obtained from competent authorities of foreign states based on agreements on avoidance of double taxation. The RF currently has 81 such bilateral agreements. Along with that, Russia has signed 11 intergovernmental agreements on cooperation and mutual assistance on tax compliance with CIS states. In 2015, the OECD Multilateral Convention on Mutual Administrative Assistance in tax matters came into effect for Russia, thereby ensuring exchange of information with 80 jurisdictions.[29]

---

[23] FATF, Interpretative Note to Recommendation 10.5.

[24] When a FI is unable to complete customer due diligence (CDD), the FATF standard provides that the FI should be required not to open the account, or to terminate the business relation, and consider making a suspicious transaction report. This contemplates situations when the identity of the beneficial owner or natural person holding the position of senior managing official cannot be verified by the FI. (FATF, Methodology 2013, Criterion 10.19).

[25] Federal Law No. 115-FZ, as amended, Article 7.

[26] Federal Law No. 115-FZ, Article 7.

[27] "De-offshorization" refers to measures to discourage Russian individuals and companies from using foreign corporate structures to conceal beneficial ownership or obtain undue tax advantages.

[28] Federal Law No. 376-FZ (November 24, 2014).

[29] The RF currently has 80 such agreements. (Available via the Internet: https://www.nalog.ru/eng/international_cooperation/dta/).

21. None of the current systems in the RF achieves adequate transparency regarding the beneficial ownership of legal persons. In the last progress report to the FATF, the authorities indicated that the FIs provided a virtual national beneficial ownership registry, since every legal person is required to have an account in a FI, and FIs are required under the amended AML/CFT law to identify the beneficial owner.[30] However, doubts remain as to whether—in implementation—the identification and verification of BO information by FIs are effective and adequately robust. BO information collected by FIs through the customer due diligence process is not always available, up-to-date, or accurate when requested by concerned agencies.

22. Nevertheless, the authorities are undertaking steps to address the shortcoming. A bill has been submitted to the parliament that would require all legal entities to keep and periodically update beneficial ownership information within their principal office, and to provide such information at the request of the Rosfinmonitoring or other authorized federal executive body.[31] The bill would also allow for the imposition of administrative liabilities and fines in cases where legal entities fail to comply with these requirements.

23. The authorities did not provide information on sanctions that have been imposed on FIs for failure to comply with the requirements regarding the identification of beneficial ownership. Such data could have provided context to FIs' implementation with their obligations on beneficial owner information.

C. Access to Beneficial Ownership Information by Relevant Concerned Agencies

24. The Rosfinmonitoring, FTS, and Law Enforcement Agencies (LEAs) have timely access to basic information of legal persons and bank accounts held by natural and legal persons. Through the taxpayer identification number, the FTS has timely access to accounts held by natural and legal persons. LEAs and Rosfinmonitoring can also access such information with the FTS.

25. However, LEAs' actions to access BOs information is limited. STRs and CTRs collected by Rosfinmonitoring could give LEAs an indication of the BO information. However, since the banks' identification of BOs is not always thorough, the BO information contained in STRs filed with Rosfinmonitoring is likely to be of limited value. Furthermore, LEAs make little use of special investigative techniques to locate the ultimate beneficial owners of companies. Often the investigations' starting point is whatever information is publicly available in the USRLE, which all LEAs have access to. In some cases, mutual legal assistance has to be sought to trace BO information across borders and the authorities indicated this can, on occasion, prove challenging or slow, and that it is not used very often.

[30] FATF, Russian Federation: 6th Follow-Up Report (October 2013).

[31] Bill No. 96535-6 (A bill on amendments to certain legislative acts of the Russian Federation with regard to the establishment of obligations of legal entities to disclose their beneficial ownership).

D. Conclusions and Recommendations

26. The authorities should continue taking concrete steps to improve the availability of beneficial ownership information of legal persons in the RF. It is recommended that the authorities conduct a comprehensive assessment (through the NRA, if possible) to obtain a more granular understanding of the risks of legal persons being misused for ML and TF. The authorities should ensure that banks are properly identifying their customer's beneficial owner and verifying their identity. CBR and Rosfinmonitoring should provide further guidance and education to banks on steps needed to identify the ultimate beneficial owner of a customer, and clarify that reliance on the customer's self-declaration is not, in itself, sufficient—FIs should instead verify the information independently without relying on the customer. Effective implementation of strengthened requirements on beneficial ownership information, including the imposition of penalties for non-compliance, should be enhanced. The draft bill establishing requirements for legal entities to provide and disclose beneficial ownership information is a positive step; however, its effective implementation is paramount. Finally, the authorities could consider—as an alternative to the draft bill—creating a public registry for beneficial ownership information.

PREVENTIVE MEASURES—POLITICALLY EXPOSED PERSONS AND REPORTING OF SUSPICIOUS TRANSACTIONS

A. Politically Exposed Persons—Measures in Banks

27. The issue of domestic politically exposed persons (PEPs) is of particular concern to banks in the RF, reflecting corruption across the public sector. Banks in the RF are required to take reasonable measures to identify foreign and domestic PEPs, and officials of public international organizations. Such measures include securing management approval before establishing business relationships with PEPs, identification of the sources of funds or origins of their monetary assets or property, regularly updating information on such persons,[32] and paying special attention to transactions made by PEPs and their family members.[33]

28. However, the definition of PEPs in the AML/CFT law falls short of the FATF standard and there are some shortcomings in measures for addressing their ML risks. The definition of PEPs under the AML/CFT law appears to limit the scope to public officials appointed by the President. For instance, according to the authorities, Ministers, judges, senior executives of state owned corporations, and senior military officials are appointed by the President. However, important political party officials, and senior politicians are not, and would, thus, be outside the law's definition of PEPs. Furthermore, the reference to the parliamentarians is made indirectly, since the PEP definitions only refers to the members of committees and commissions of the Parliament and

[32] Federal Law No. 115-FZ, as amended, Article 7.3.

[33] Federal Law No. 115-FZ, as amended, Article 7.3.

according the Regulation of State Duma, all parliamentarians must be members of committees and commissions. In compliance with the FATF standards, the scope of PEPs to be covered should be based on the prominent public functions that an official is entrusted with, rather than the appointing power.[34] The restrictive definition can restrain banks' application of enhanced due diligence measures and hence, increase their risks of failing to identify and report suspicious transactions of high-level public officials (not appointed by the President). Moreover, the AML/CFT law needs to be clarified to ensure that enhanced measures apply not just to customers who are identified as PEPs, but also beneficial owners of customers who are PEPs. Finally, banks are only required to pay special attention to transactions of PEPs and their family members, but not of close associates or PEPs who are beneficial owners as prescribed by the revised FATF standard.

29. The gaps in the preventive measures against PEPs consequently affect the banks' effectiveness in addressing ML risks from PEPs. AML/CFT supervision of banks' compliance of PEP requirements will be limited and may not ensure that banks are effectively monitoring ML risks of PEPs. Owing to the gaps, only a small percentage of customers have been identified by banks as PEPs. The low identification rate of PEPs may be due to the bank's inadequate understanding or capacity to identify customers as PEPs, aside from the limited definition under the law. Furthermore, no data was provided by authorities on sanctions for violations by FIs of requirements regarding PEPs.

30. Enhancing the requirements for domestic PEPs, and supervision could assist anti-corruption efforts. The authorities should bring the definition of and measures for PEPs in line with the FATF standard. Guidance from relevant supervisors on identifying PEPs, family members as well as close associates, and PEPs who are beneficial owners, and best practices in implementation of preventive measures can assist banks in strengthening their systems. Finally, CBR inspections do not focus sufficiently on the level of compliance and adequacy of banks in implementing the PEP requirements in line with the standard.

B. Suspicious Transaction Reports

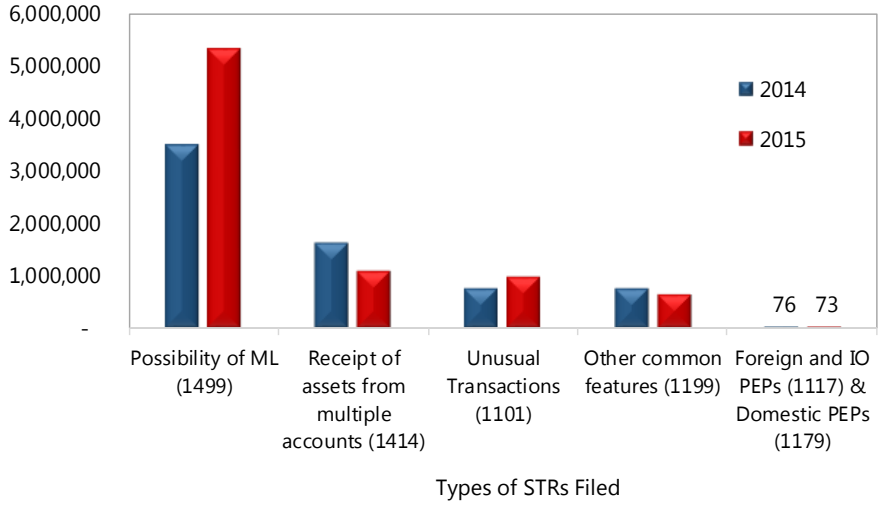
31. The requirements for financial institutions to report suspicious transactions appear to be in line with the revised FATF standard. Under the revised FATF standard, if a FI has reasonable grounds to suspect that funds are proceeds of a criminal activity, or are related to terrorist financing, then it should be legally required to promptly report its suspicions to the financial intelligence unit. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction. FIs are required to submit to Rosfinmonitoring information on transactions for which there is a suspicion that they are carried out for ML/TF purposes and

[34] Foreign and domestic PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country or domestically (respectively), for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

transactions subject to compulsory control (in excess of RUB 600,000).[35] Attempted transactions of customers with an existing business relationship and of occasional customers are covered.[36]

32. Rosfinmonitoring receives a large volume of reports of suspicious transactions, but disproportionately few reports on PEPs (Figure 1). In 2014, Rosfinmonitoring reported receiving over 11 million suspicious transaction reports (STRs) with an estimated value of RUB 160 trillion (most of which were sent by credit institutions).[37] The number of criminal cases initiated based on the information provided by Rosfinmonitoring has reportedly risen from 500 in 2013 to 1,500 in 2014.[38] Of the 11 million STRs in 2014, those filed on the sole basis of suspicions by reporting entities amounted to more than six million in 2014 and rose to eight million in 2015. Total STRs filed with respect to PEPs (foreign, domestic and international organizations) was less than 100 in both years with is not commensurate with the related risks.

Figure 1. Suspicious Transaction Reports



Source: Rosfinmonitoring.

33. The FI's suspicious transaction reporting system to Rosfinmonitoring appears to be functioning well. A single telecommunications network is provided to FIs, in which to submit STRs. The automated system filters incoming STRs, and rejects improperly generated STRs for return to the sending FIs. In addition, Rosfinmonitoring publishes newsletters to clarify issues related to the filing and sending of STRs to guide reporting entities, and typology reports on schemes or suspicious

[35] See also CBR Regulations No. 321-P.

[36] See MONEYVAL, Russian Federation: Progress Report (September 16, 2014), page 17, paragraph 89.

[37] Rosfinmonitoring, Activity Report (2014), p. 14.

[38] The main targets of these cases involved public procurement (24 percent), financial sector (17 percent) and corruption (13 percent).

transactions in relation to ML/TF activities. Rosfinmonitoring sends some of the collected information to the CBR, as regards potential violations of STR regulations by reporting FIs. The CBR also uses the information in the framework of its supervisory activities, with the aim of discussing with FIs efforts to improve the quality of STRs.

34. CBR predetermined criteria—which in some cases may not be comprehensive enough to cover all potential ML/TF risks—might not leave room for the appreciation of suspicious transactions by banks. The transmission system does not seem to provide much flexibility for FIs to assess suspicious transactions. Instead, it over relies on predetermined criteria that are provided and updated regularly by the CBR. CBR inspections are very focused on the reporting framework, and the level of compliance of banks to reporting in line with the predetermined criteria. Several sanctions (including revocation of licenses) were imposed because banks failed to report suspicious transactions that were later determined to be suspicious by the CBR. Such systems can also lead to over-reporting or defensive-reporting. Moreover, criteria provided by the CBR demonstrate some shortcomings in terms of scope and do not necessarily cover all possible scenarios of suspicious transactions.

35. Rosfinmonitoring is of the general view that significant improvement has been made in the quality of the STRs that it has received from the banking sector in recent years, but the STRs do not appear to correlate with the RF's ML/TF risks. It is not clear to what extent the STRs filed with Rosfinmonitoring reflect the RF's ML/TF risk profile. The STRs relating to PEPs are not commensurate with the ML risks, and most of the reports concern unusual transactions rather suspicions of the laundering of proceeds of crimes.

36. Rosfinmonitoring in consultation with CBR provides good quality general guidance on STRs, but could improve case-by-case feedback to FIs. More case-by-case feedback about the STRs and their outcome (e.g., closed, disseminated) would assist FIs in improving the quality of their STRs.

C. Conclusions and Recommendations

37. The authorities should ensure that the definition of PEPs is fully in line with the FATF standard. Guidance should be provided to FIs to assist them in identifying and dealing with PEPs (including beneficial owners, family members, or close associates).

38. Rosfinmonitoring, in coordination with CBR, should provide additional guidance and timely feedback to FIs on the reporting of suspicious transactions. Sufficient guidance and case-by-case feedback will help improve the quality and timeliness of reporting by FIs, and their understanding of fraud, corruption, and tax evasion typologies. When completed, the results of the NRA should be shared with the FIs to improve their understanding of and the quality of their suspicious reports to align them further with the ML/TF risks in Russia.

AML/CFT SUPERVISION—RISK BASED APPROACH AND SANCTIONS

A. Supervision of Banks Based on Risks

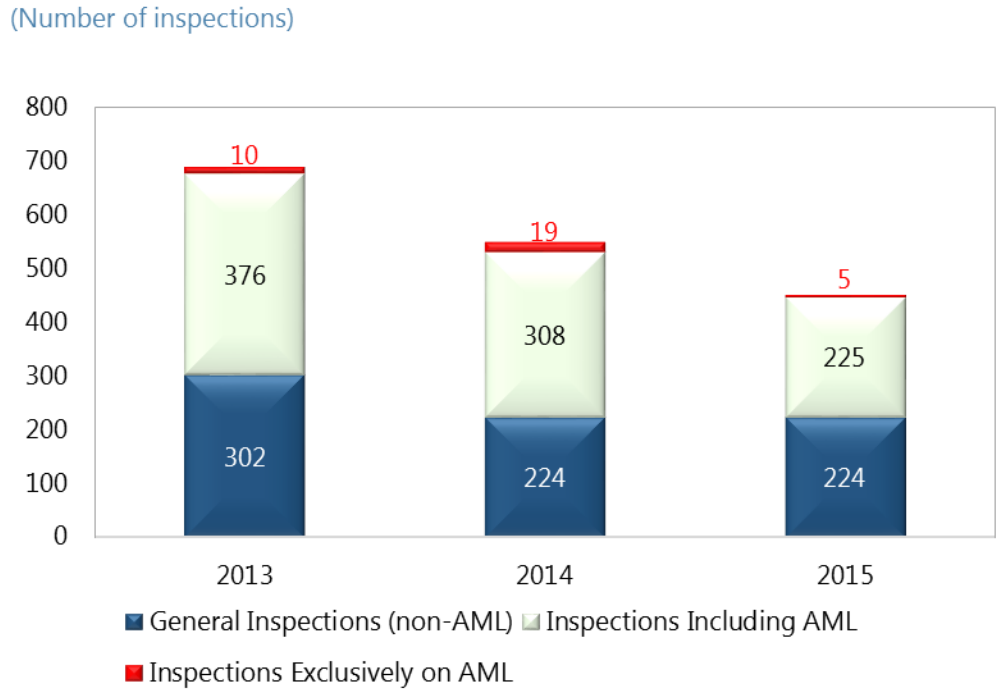
39. Since the last assessment, the CBR has made a significant effort to enhance the AML/CFT supervision of banks. The size of the country's territory as well as the large number of licensed institutions create significant challenges for supervisory authorities. At the time of the 2008 comprehensive assessment, the FATF found the AML/CFT supervision of FIs, the sanctioning powers and the sanctions themselves to be inadequate.[39] The resources of the CBR have since been increased, including through a merger with supervisors of the Federal Service that has allowed it to have a three years' inspection cycle. As a result, the FATF concluded in the 2013 progress report that the technical requirements for supervision and sanctions were largely in line with the previous standard and methodology.

40. The authorities apply a risk-based approach to AML/CFT supervision of FIs, but the tools could be further improved. The CBR relies on the regular analysis of the 17 reporting forms from banks (see Annex I), information gathered from Rosfinmonitoring on the level of STR, and LEAs' investigations as well as analysis of its internal databases and direct contacts with FIs to target its AML/CFT inspections. The CBR gives undue reliance on risk mitigation based on a checklist of predetermined criteria, rather than on a robust analysis of indicators of inherent ML/TF risks of banks. CBR offsite activity is centered on the review of the 17 categories of reporting, but the information on the ML/TF risks of the sector, risk profiles of the individual institutions, and their level of AML/CFT compliance are insufficient.

41. CBR risk based inspections could be enhanced further. Supervisors regularly conduct scheduled and unscheduled on-site inspections. From 2013 to 2015, more than half of all total scheduled inspections included AML/CFT issues, with several inspections devoted exclusively to AML/CFT concerns (Figure 2). In addition, approximately 20% of all unscheduled inspections involved AML/CFT issues (Figure 3). However, the CBR's understanding of risks relating to banks, and its supervisory tools could be enhanced in order to provide it with comprehensive, timely and consistent data on the nature and potential exposure to ML/TF risk (inherent risk) at the institutional level. There is no well-defined, documented methodology that integrates the findings generated by the CBR for operational risk into a rating that takes comprehensive information on inherent risk, and risk mitigants into account, in order to prioritize banks for supervisory oversight. The risk-based methodology does not seem to capture information relating to the level of compliance of AML/CFT measures in individual banks, including for instance the exposure to PEPs or weak implementation of beneficial ownership requirements.

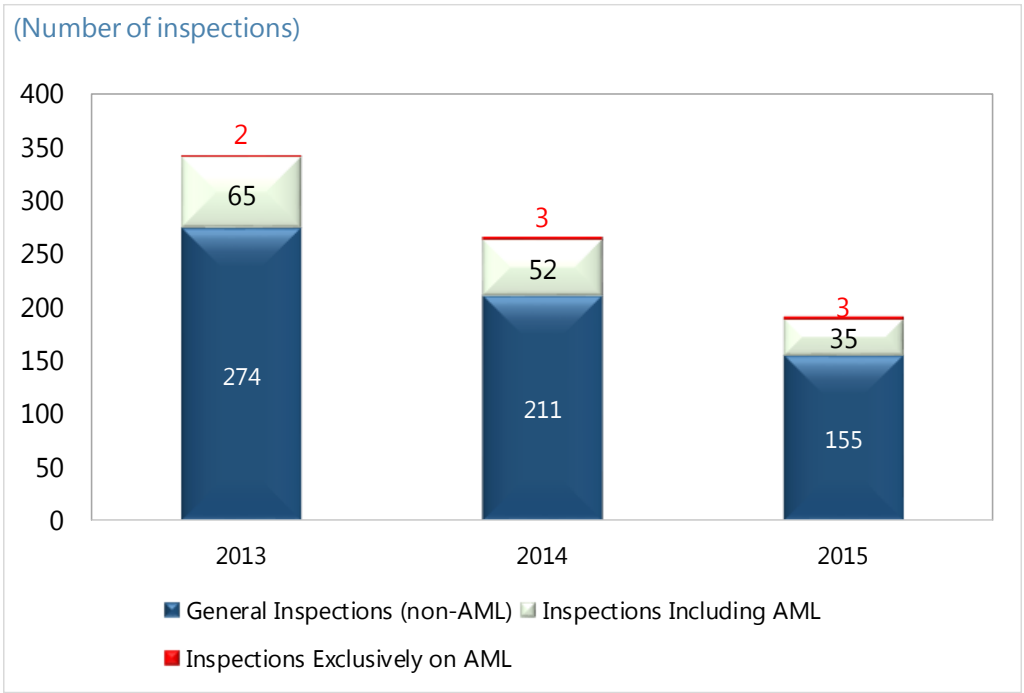
[39] FATF, 2008 MER, page 12.

Figure 2. CBR Onsite Inspections (Scheduled)



Source: CBR.

Figure 3. CBR Onsite Inspections (Unscheduled)

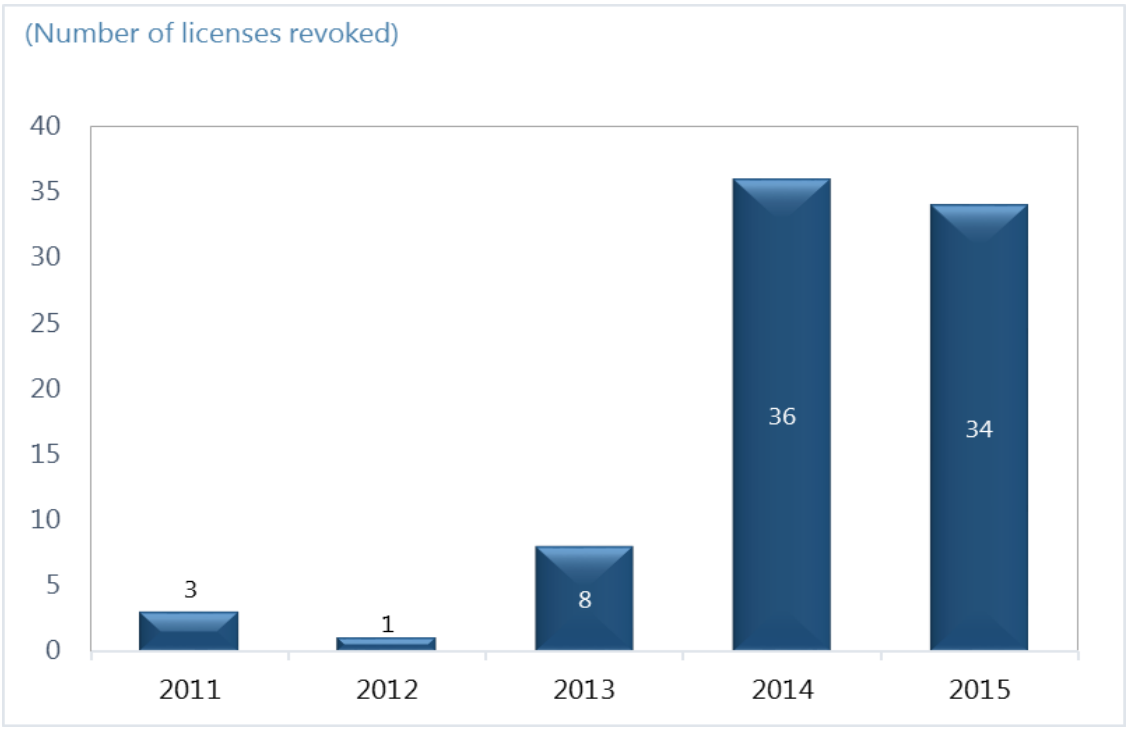


Source: CBR.

B. Sanctions

42. Efforts to revoke bank licenses owing to violations of AML/CFT requirements have ramped up in recent years. There has been a marked decrease in the number of active banks in Russia (from 1,351 as of January 31, 2006 to 945 registered banks[40]), owing to revocation of licenses, mergers and acquisitions, and unilateral decisions to close the business, among others (for more, please refer to BCP 11 assessment). Licenses revoked by the CBR due to AML/CFT violations sharply increased in 2014 (36 licenses, 11 of which were based solely on AML/CFT violations), which surpasses the total number from 2011 to 2013 (Figure 4). The trend continued with 34 revoked bank licenses in 2015, involving AML/CFT violations. The revocations involved not just the small banks, but also included the bigger banks (e.g., Master bank, AB Pushkino, MAST bank).

Figure 4. Bank Licenses Revoked due to AML/CFT Violations



Source: CBR.

43. Although the sanctions seem to be dissuasive, they should also be proportionate to the severity of the identified breaches. Among the license revocations due to AML/CFT violations, most were due to the failure of banks to report suspicious transactions. CBR should pursue a more graduated approach to sanctions. The objective is to ensure that sanctions (such as administrative fines, prohibition of certain categories of transactions, and restrictions on operations of branches,

[40] CBR website: http://www.cbr.ru/Eng/statistics/print.aspx?file=bank_system/inform_06_e.htm&pid=lic&sid=itm_46099

and revocations in extreme cases) are proportionate to the severity and frequency of the violations, or the score a bank receives as a result of the inspection.

C. Conclusions and Recommendations

45. **To enhance AML/CFT supervision of banks, the CBR should improve its understanding of ML/TF risks based on the results of its own national risk assessment**. While the risk-based supervisory methodology currently used by the CBR will improve the situation, some concerns remain about its limitations in capturing information relating to exposure to inherent ML/TF risks of banks, including those related to some clients (e.g., PEPs). Furthermore, the CBR's range of sanctioning powers should be applied in a manner that is proportionate to the severity of identified breaches or the rating assigned resulting from the inspection.

Annex I. Reporting Forms for Offsite AML/CFT Supervision of Banks

Number	Reporting form	Periodicity
1	Turnover Sheet of the Credit Institution's Business Recording Accounts.	Monthly
2	Information on the Standard of the Credit Institution's Assets (Banking Group).	Monthly
3	Report on the Cash Turnover.	Monthly
4	Information on Transactions with the Use of Payment Cards and on the Infrastructure, Intended for the Performance with or Without the Use of Payment Cards of Transactions for the Issue (Acceptance) of Ready Cash and of Payments for Commodities (Works, Services).	Quarterly
5	Information on the accounts of clients and the payments carried out through the credit organization (its branch).	Quarterly
6	Information on settlements between residents and non-residents for the performance of works, rendering of services, information transfer, results of intellectual activity, operations of a non-commercial character and for the goods that do not cross the border of the Russian Federation.	Monthly
7	Information on Operations with Securities, Stakes, Partner Shares and Deposits in the Property Made Between Residents and Non-residents	Monthly
8	Report on Operations with Foreign Money Cash and Cheques in Foreign Currency.	Monthly
9	Information on the Opened Correspondent Accounts and on the Residuals of Funds on Them.	Monthly
10	Report on currency transactions made on bank accounts and on the clients' accounts at the authorized banks.	Monthly
11	Report on Currency Transactions the Performance of Which Envisages the Formalization of the Passport of the Transaction.	Monthly
12	Report on Transactions on the Currency and Money Markets.	Daily
13	Report on Securities.	Monthly
14	Bank Control Record on the Contract (also see appendix 6 to Instruction of the CBR №138-I).	Monthly
15	Report on Observance of Foreign Exchange Control legislation by credit institutions and AML/CFT legislation by credit institutions and non-credit FI (submitted by CBR territorial units).	Irregular basis (when information is available)
16	Information on types and volume of transactions conducted by non-credit financial institutions.	Monthly
17	Report on off-exchange transactions.	Monthly