Executive Summary

1. This report summarises the AML/CFT measures in place in the Russian Federation (hereafter referred to as Russia) as at the date of the on-site visit (11-29 March 2019). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Russia's AML/CFT system, and provides recommendations on how the system could be strengthened.

Key Findings

1. Rosfinmonitoring is core to the functioning of Russia's AML/CFT regime, as it is responsible for leading and co-ordinating policy and operational activities in the field of AML/CFT. This work is strongly supported, including legislatively, as AML/CFT is afforded the highest priority by the Russian government. Domestic co-ordination and co-operation is a major strength of the Russian AML/CFT system.
2. Russian authorities have an in-depth understanding of the country's ML and TF risks, as outlined in Russia's 2018 ML and TF NRAs and communicated by authorities to the assessment team. Both ML and TF risks are well identified and understood by all authorities. FIs have a good understanding of these risks, while other reporting entities' understanding varies.
3. Rosfinmonitoring has a wealth of available data, including a large volume of reporting, and employs sophisticated technologies and high degree of automation, to prioritise, generate, and contribute to investigations pursued by law enforcement authorities (LEAs). LEAs routinely and effectively access and use this financial intelligence to investigate ML, TF, predicate offenses, and to trace criminal proceeds. Prosecutors further ensure the use of financial intelligence in case development by systematically reviewing investigations to verify that LEAs pursue all financial aspects.
4. Russia is investigating ML partly in line with its risk profile. LEAs routinely conduct financial investigations alongside predicate offences. Most ML investigations involve the acquisition or sale of criminal proceeds, so the majority of cases relate to less serious offences. Self-

laundering is frequently investigated, unlike third-party ML, which is detected and investigated to a lesser extent. Some complex ML is pursued, however more opportunities for LEAs to uncover and investigate sophisticated and/or high-value ML may exist, especially in the financial sector and involving proceeds sent abroad, particularly those related broadly to corruption. Sanctions applied against natural persons for ML are moderately effective, and while Russia cannot prosecute legal persons, the use of administrative sanctions against legal persons was not demonstrated. Alternative measures are a notable part of Russia's toolkit to combat financial and shell company-related offences potentially related to ML.

5. Russia has a robust legal framework for combatting TF, which is largely in line with international standards. On average, Russia pursues 52 TF prosecutions per year. Since 2013, Russia has convicted more than 300 individuals of TF, with the majority resulting in sentences of imprisonment ranging from 3-8 years. Russia demonstrates that it deprives terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities through various approaches, such as through terrorist designations, administrative freezes, court orders, and confiscation. While the total amount of assets and instrumentalities deprived is relatively low, this is consistent with Russia's risk profile.

6. Overall, Russia has an adequate system to implement TF and proliferation financing (PF) targeted financial sanctions (TFS), but has gaps and weaknesses in some areas, including TFS implementation without delay and a lack of explicit, legally enforceable requirements that extend to all natural and legal persons (beyond reporting entities).

7. There is a widespread and persistent trend of non-compliance with preventive AML/CFT obligations particularly in the financial sector. Although breaches have been decreasing in recent years, the absolute figures are still worrisome. The threshold for suspicious transaction reporting is low and automation in filing leads to a massive number of reports, which, while used in the FIU's datamining, are not detailed or suited for flagging a high level of suspicion or urgency. This increase in STRs could be leading to more terminations of business relationships and refusals to conduct transactions due to ML/TF concerns. Group-wide information sharing among FIs was not possible in Russia until the on-site visit.

8. The Bank of Russia (BoR) has implemented some aspects of risk-based supervision since 2013, and has recently improved the risk-based approach to supervision. Licensing requirements for FIs were strengthened in 2013 and now largely mitigate the risk of criminals being the owners or the controllers of FIs. However, supervision is mostly based on prudential factors and the BoR over- relies on remote monitoring. While a number of licence revocations have occurred, sanctions are not effective or dissuasive in all cases and monetary penalties imposed are low.

9. Russia has improved its legal framework and operational approach to enhance transparency of legal persons, which makes it more difficult to misuse a legal person established in Russia. Registration requirements have been enhanced and legal persons are constantly being reviewed and removed for providing inaccurate information or for inactivity. Legal persons maintain information on their beneficial owners and authorities effectively supervise the implementation of this requirement. FIs and DNFBPs also collect beneficial ownership information of customers, but have somewhat limited capacity to verify it.

Risks and General Situation

2. Russia is generally perceived as a source country for proceeds of crime, and is not a major centre for laundering the proceeds of crime committed in other countries. Nevertheless, Russia is exposed to a wide range of ML risks.

3. Russia has conducted NRAs for ML and TF. Assessors largely agree with the results. The ML NRA identifies embezzlement of public funds, crimes related to corruption and abuse of power, fraud in the financial sector, and drug trafficking as the prevalent types of criminal activity with the potential to generate illicit proceeds. A large proportion of criminal proceeds generated in Russia are laundered abroad, as recognised by the ML NRA, which makes the pursuit of proceeds of crime to other countries an important focus for the assessment. The assessment team also considered the risks associated with organised crime and cyber-crimes, which occur alongside the threats identified in the NRA.

4. Russia is not a global financial centre, but does have a significant banking sector primarily serving domestic customers and including many small banks. The sector has undergone significant structural changes in recent years primarily driven by supervisory actions – through closures, mergers, and acquisitions – which has halved the number of active banks. The assessment team looked at the reasons for this consolidation and its impact on how well the sector implements preventive measures against ML and TF.

5. The main TF risks in Russia relate to foreign terrorist fighters (FTFs) destined for and returning from ISIL-controlled areas of Iraq and Syria, but Russia also faces domestic terrorist threats. The assessment team reviewed the measures taken to combat all terrorist threats and associated financing, including the remaining threat posed by armed groups in the North Caucasus.

Overall Level of Compliance and Effectiveness

Assessment of risk, co-ordination and policy setting (Chapter 2; IO.1; R.1; 2; 33 & 34)

6. Russian authorities have a very developed understanding of the country's ML/TF risks. Identification and assessment of ML/TF risks is done as a systemic exercise, which benefits from the high-level political commitment and the participation of all major stakeholders from both the public and the private sectors. The ML NRA uses a large amount of quantitative and qualitative data from a multiplicity of public

and non-public sources. The methodology of the ML NRA is generally sound, although some improvements could be made.

7. The ML risks identified seem comprehensive and reasonable. The authorities met on-site demonstrated advanced understanding of and clear views on the constituents of risk, are aware of the most relevant countrywide and sector-specific risks, including the applicable risk scenarios, methods and tools.

8. TF risks are well identified and understood. The TF NRA is high-level and does not provide granular information about specific threats. Nevertheless, it is usefully supplemented by the in-depth knowledge of the criminal intelligence and investigation staff of the LEAs involved in counter-terrorism. Rosfinmonitoring has a key role in identification of TF-related threats and generation of relevant intelligence output.

9. National AML/CFT policies appropriately address identified ML/TF risks. There is an on-going and consistent policy development process in Russia, which builds on the outcomes of formal risk assessments and other articulations of risks (such as the annual threat assessment reports produced by Rosfinmonitoring since 2013). Relevant national strategies and ML and TF action plans derived from the outcomes of 2018 NRAs represent the national policies at the strategic and operational levels aimed at combating ML/TF in the country. Domestic co-ordination and co-operation is a major strength of the Russian AML/CFT system.

Financial intelligence, ML investigations and prosecutions, and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

10. Russian LEAs routinely and effectively access and use financial intelligence and other relevant information to develop evidence to investigate ML, TF, predicate offenses, and to trace criminal proceeds. Prosecutors further ensure the use of financial intelligence in case development and they systematically review investigations to verify that LEAs pursue all financial aspects.

11. Rosfinmonitoring is core to the functioning of Russia's AML/CFT regime. Rosfinmonitoring has a wealth of available data, including a large volume of STRs (20 million per year, on average) and MCRs (another 10 million per year, on average). It employs sophisticated technologies and a high degree of automation, to prioritise, generate, and contribute to cases pursued by LEAs. Rosfinmonitoring is a well-resourced and data-driven FIU with competent analysts that has a uniquely wide view into the Russian financial system.

12. To a large extent, Rosfinmonitoring's financial analysis and dissemination support the operational needs of relevant LEAs. LEAs also demonstrated that the financial intelligence either received from Rosfinmonitoring, spontaneously or upon their request, is of high quality and integral to their activities.

13. Rosfinmonitoring's close co-operation and co-ordination with its domestic counterparts greatly contributes to Russia's effectiveness.

14. ML is generally well identified through financial investigations, and when it is identified, the authorities open ML investigations in more than 91% of instances, with most cases resulting in charges. LEAs routinely conduct financial investigations when looking into predicate offences, but usually do not pursue ML outside of

predicate investigations. Self-laundering is frequently investigated, unlike third-party ML, which is detected and investigated to a lesser extent. The investigative process is rather formal, which brings efficiency and productivity, but ML investigations may not be opened or completed when there is evidence of a more easily provable alternative charge.

15. Russia is investigating ML activity partly in line with its risk profile, as approximately 85% of ML offences detected related to the high-risk areas denoted in the NRA, such as drug crimes and crimes with public funds. In the area of bribery, the number of ML cases pursued is not entirely aligned with risk, even though there are many corruption predicate investigations and thousands of recent convictions. While Russia is investigating and prosecuting offences stemming from some notorious, multinational laundromats, including by investigating complicit professionals in the financial sector, the authorities are not sufficiently targeting bankers who facilitate ML.

16. Sanctions applied against natural persons for ML are partly effective, proportionate, and dissuasive, as terms of imprisonment for ML and fines are on the low-end, with some exceptions. Per fundamental principles, Russia cannot prosecute legal persons, but the use of administrative sanctions against legal persons was not demonstrated.

17. Russia beneficially employs alternative measures to prosecute financial crimes that could be indicative of, or occur in connection with, ML activity. These offences do not necessarily involve proceeds of crime and it is not always apparent why ML investigations or charges are not simultaneously pursued. The most impactful alternative offence used is illegal banking, followed by the outflow offence and offences related to shell companies. These measures disrupt schemes that may represent third-party ML infrastructure. However, they require less investigation into the full scope of the criminal conduct and may not be as easily recognised by other countries when co-operation is sought.

18. Russia pursues confiscation as a policy objective and traces the proceeds and instrumentalities of crime. Provisional measures are used well, including for equivalent value. The overall statistical picture on many of the facets of confiscation, broadly defined, is solid.

19. Authorities focus on compensating victims, so restitution figures are higher than criminal confiscation figures. This is appropriate in the Russian context where many offences in the high-risk areas of crimes with public funds, as well as financial sector crimes such as fraud, embezzlement, and misappropriation, have identifiable victims. Restitution is the priority and criminal confiscation is used when legal owners cannot be identified or for offences that create proceeds but do not cause pecuniary loss. Confiscation of the unexplained wealth of public officials is showing more results year over year.

20. Confiscation regarding falsely or non-declared movements of currency and bearer negotiable instruments (BNI) is pursued to a lesser extent, partly due to the lack of a declaration obligation within the Eurasian Economic Union (EAEU). Considering Russia's vast land borders and other relevant risk and context, a relatively low percentage of smuggled cash that is identified is confiscated. However, detected smuggling offences and imposed fines appear to partly offset these limited confiscations.

21. Russia recognises the threat posed by the misuse of virtual assets (VA), especially as related to drug trafficking and internet-enabled crime. LEAs can trace but cannot confiscate virtual assets until they are exchanged into property, as legally defined, and while some ML cases have featured VA, an ML charge cannot yet be solely based on transactions involving VA.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4–8; 30-31; and 39)

22. Russia has a robust legal framework for combatting TF, which is largely in line with international standards.

23. LEAs and prosecutors must consider in the course of each criminal investigation whether there are indications of other crimes and whether property has been used or intended for use to finance terrorism or groups engaged in such activity. This requirement has the effect of ensuring that the investigation of the financial aspects of terrorist crimes is mandatory. In practice, LEAs systematically consider the financial component of terrorist activities, which had led to the detection, identification and investigation of TF. Russia is able to identify different methods of TF and the role played by financiers.

24. On average, Russia pursues 52 TF prosecutions per year. Since 2013, Russia has convicted more than 300 individuals of TF, with the majority of cases resulting in sentences of imprisonment ranging from 3-8 years.

25. Russia demonstrates that it deprives terrorists, terrorist organisations and terrorist financiers of assets and instrumentalities through various approaches, such as through terrorist designations, administrative freezes, court orders, and confiscation. While the total amount of confiscated assets and instrumentalities is relatively low, this is consistent with Russia's risk profile.

26. Overall, Russia has an adequate system to implement TFS, but major gaps and weaknesses exist in some areas, including TFS implementation without delay and a lack of explicit, legally enforceable requirements that extend to all natural and legal persons (beyond reporting entities).

27. Russia's domestic TFS regime has both terrorism and extremism activity as potential grounds for designation. The process for accessing frozen funds differs between the "international" list (which relates to UN designations) and the domestic list. As a result, the assessment team noted confusion among reporting entities met on-site regarding the various lists (UN lists, domestic terrorism list, domestic extremism list) and their respective procedures to seek special exemptions or access to frozen funds.

28. While Russia identified the overall TF risk associated with NPOs as low, some parts of the sector were assessed as medium-risk and subject to additional controls. Russian authorities are conducting risk-based outreach to and supervision of NPOs.

Preventive measures (Chapter 5; IO.4; R.9–23)

29. FIs have procedures in place to identify, assess, understand and document their individual risks, including through a periodic risk assessment exercise. FIs have implemented adequate mitigation measures by profiling their customers based on ML/TF risks and applying adequate measures for CDD, record-keeping and monitoring.

30. Overall, there is a fair level of implementation of the requirements among FIs related to the identification of BO, but some FIs apply a rules-based definition of BO (i.e. identifying senior management officials as soon as no natural person is identified as owning 25% or more of legal persons). This may be due to a superficial understanding of the definition of BO.

31. The understanding of risks by DNFBPs, as a whole, is fair. Certain sectors have a good understanding (e.g. accountants and auditors). Others have a less developed (casinos, real estate agents) or superficial (lawyers and notaries) risk understanding. Risk understanding by DPMS is not considered to be in line with the risk identified in the ML NRA.

32. DNFBPs rate customers based on ML/TF criteria and apply CDD and EDD measures accordingly. While DNFBPs are aware of their STR obligations, few are filing an adequate amount of STRs.

Supervision (Chapter 6; IO.3; R.14; 26–28; 34-35)

33. The banking sector is exposed to a high level of threat from criminals. Since 2013, the number of credit institutions (CIs) licenced in Russia was halved due to mergers and the revocation of many licences (including for serious violations of AML/CFT provisions). The licensing requirements for FIs has improved since 2013 and now largely mitigate the risk of criminals being the owners or the controllers of FIs; however, deficiencies in licensing remain.

34. Since 2013, the Bank of Russia (BoR) has put in place an intense bank supervisory programme informed by AML/CFT risks. Planned on-site inspections follow a time-bound cycle, to which AML/CFT components can be added. Targeted (ad hoc) inspections, solely focused on AML/CFT can be organised, however, few have been carried out. BoR has shifted its supervisory strategy from on-site inspections to remote supervision, which uses algorithms to identify possible involvement in suspicious transactions and detect potential AML/CFT breaches. Assessors are concerned that an insufficient number of on-site inspections for AML/CFT issues is taking place, and consider that the current BoR supervision model over-relies on remote forms of supervision. AML/CFT supervision for non-credit FIs has only recently moved to a risk-based approach and the resource allocation to sectors is not fully in line with sector risks.

35. Overall compliance by FIs has improved in recent years. A significant number of licence revocations for serious AML/CFT violations has had a cleansing effect. However, monetary penalties imposed for AML/CFT breaches are relatively low.

36. Roscomnadzor and DNFBP supervisors have their own risk assessment methods, however, the ML/TF risk understanding was largely improved after the NRA process. Rosfinmonitoring has conducted AML/CFT specific on-site and off-site inspections of DNFBPs under its remit using a risk-based approach. Other DNFBP

sectors undergo supervision for prudential and conduct of business purposes, which can include AML/CFT issues. Supervision of the DPMS sector should be more focused on AML/CFT compliance, based on a comprehensive understanding of risk exposure, including as identified in by the NRA.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

37. The risk of misuse of legal persons in ML schemes is high. Russia has put in place a number of mechanisms that significantly mitigate the misuse of legal persons for ML/TF purposes. In particular, there are stringent rules at registration, and since 2017, authorities have strengthened measures to identify inaccurate information and inactive companies. As a result, the accuracy of the company register (the USRLE) has improved, which makes its information more useful for LEAs and others.

38. The company register is mainly source of legal ownership information, but it can be a source of BO information where (i) all the shareholders are in the register and (ii) no doubts arise as to other persons being the BO. Credit institutions are also a source of BO information, although the verification of information by reporting entities is largely based on the company register, which may not always hold BO information. A challenge exists in relation to accessing accurate BO information when a foreign person owns a Russian legal person.

39. There is a good co-operation in investigative activities between the Federal Tax Service (FTS) and Rosfinmonitoring, as well as between FTS and LEAs. This has resulted in a large number of administrative and criminal sanctions, which contribute to making legal persons less attractive to criminals. The sanctions have, however, a limited range and level of dissuasiveness.

40. TCSPs are not considered as a distinct economic activity and are not covered by the AML/CFT law. While services provided to companies are tightly regulated, they are not properly supervised. Certain legitimate corporate services are provided, in particular by legal professionals. Legal professionals are AML/CFT obliged entities, yet they are not properly supervised and, as such, cannot be relied upon to hold adequate, accurate and current basic or BO information.

International co-operation (Chapter 8; IO.2; R.36–40)

41. In general, Russia provides mutual legal assistance (MLA) in a constructive and timely manner and swiftly executes extradition requests. Russia prioritises its responses based on the urgency indicated by the requestor, whether the request corresponds with the risks identified in the ML/TF NRAs, and legal constraints on detention of persons. An electronic case management system for the entirety of GPO assists in controlling the execution of incoming requests. Formal co-operation appears to function well in practice. Feedback on MLA and extradition as provided and sought by Russia was mainly positive.

42. Co-operation provided by Russia pertaining to asset tracing appears to be adequate. The majority of Russian requests to identify assets stem from ML investigations and the number of requests for asset identification and seizure are beginning to keep pace with suspected proceeds moved offshore.

43. Rosfinmonitoring co-operates well with foreign FIUs. To facilitate the exchange of information, it has concluded more than 100 international co-operation

agreements and is able to co-operate on basis of reciprocity. Egmont mechanisms are used for information exchange, along with other protected channels (e.g. diplomatic), and, where necessary and practicable, face-to-face meetings with foreign counterparts.

44. There are mechanisms for supervisory co-operation by the BoR, including over 30 agreements with counterparts. In its capacity of mega-regulator for the financial sector, the BoR co-operates with foreign central banks and financial regulators, but sustained relationships have not yet been developed.

45. Russia provides information on basic and BO information of legal persons. Requests for BO information comprise a relatively modest share within the total number of incoming ML requests. The authorities suggest that Russian legal persons are rarely used in foreign ML schemes and have a simple ownership structure, which diminishes the frequency of such requests.

Priority Actions

1. Russia should refine its supervisory approach to ensure that it is sufficiently ML/TF risk sensitive and independent from prudential supervision for both FIs and DNFBPs. In particular, financial supervisors should schedule sufficient AML/CFT inspections and more frequent unscheduled inspections when merited. Off-site supervision should be modified by developing more sensitive means to determine the risk profile of individual supervised institutions.
2. LEAs and prosecutors should prioritise the investigation and prosecution of complex money laundering, including professional ML linked to proceeds generated in Russia and transferred for further laundering abroad.
3. In investigating shadow financial schemes, authorities should ensure that the sources of funds and potential links to predicate offences are fully analysed. Authorities should continue to use effective alternative offences when warranted, but pursue ML investigations and consider whether a third-party ML charge is more appropriate, especially in cases where using the ML offences may facilitate international co-operation.
4. Russia should take action to implement TFS without delay and require all natural and legal persons within Russia to freeze assets and not make any funds, financial assets or economic resources available for the benefit of UN designated persons or entities, whether directly or indirectly.
5. Russia should consider ways to strengthen obliged entities' understanding of BO requirements and their implementation, particularly to identify legal persons owned or controlled by sanctioned entities, namely through complex structures, in order to detect possible instances of PF sanctions evasion.

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings[1]

IO.1 - Risk, policy and coordination	IO.2 International cooperation	IO.3 - Supervision	IO.4 - Preventive measures	IO.5 - Legal persons and arrangements	IO.6 - Financial intelligence
Substantial	Substantial	Moderate	Moderate	Substantial	High
IO.7 - ML investigation & prosecution	**IO.8 - Confiscation**	**IO.9 - TF investigation & prosecution**	**IO.10 - TF preventive measures & financial sanctions**	**IO.11 - PF financial sanctions**	
Moderate	Substantial	High	Moderate	Moderate	

Technical Compliance Ratings[2]

R.1 - assessing risk & applying risk-based approach	**R.2** - national cooperation and coordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
LC	C	LC	LC	LC	PC
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
PC	LC	C	LC	LC	PC
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
LC	LC	C	PC	LC	LC
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
LC	C	LC	LC	LC	LC
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
PC	LC	LC	LC	C	LC
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
C	LC	C	LC	LC	LC
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international cooperation		
LC	LC	LC	LC		

1 Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

2 Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.