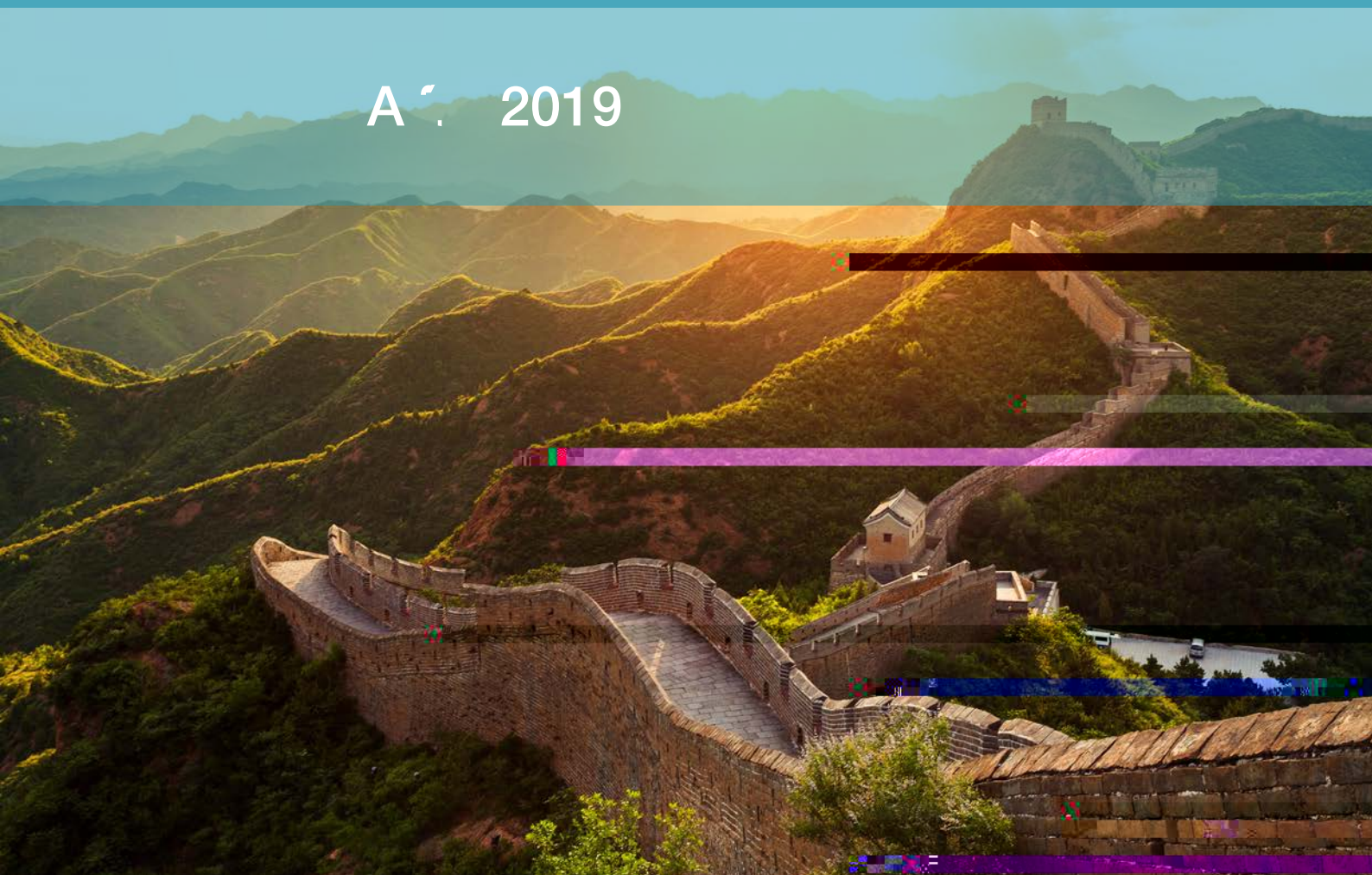
Anti-money laundering and counter-terrorist financing measures

People's Republic of China

M a E a a R

A 2019



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website:

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Citing reference:

FATF (2019), Anti-money laundering and counter-terrorist financing measures – People's Republic of China,
Fourth Round Mutual Evaluation Report, FATF, Paris
http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-china-2019.html

© 2019 FATF-. All rights reserved.
No reproduction or translation of this publication may be made without prior written permission.
Applications for such permission, for all or part of this publication, should be made to
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France
(fax: +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

Photo Credit - Cover: © Getty Images

Table of Contents

Key Findings....5
Risks and General Situation....6
Overall Level of Effectiveness and Technical Compliance....7
Priority Actions....14
Effectiveness and Technical Compliance Ratings....16

MUTUAL EVALUATION REPORT....19

Preface....19

CHAPTER 1. ML/TF RISKS AND CONTEXT....21

ML/TF Risks and Scoping of Higher-Risk Issues....22
Countryôs Risk Assessment and Scoping of Higher Risk Issues....26
Materiality....27
Structural Elements....28
Background and Other Contextual Factors....28

CHAPTER 2. NATIONAL AML/CFT POLICIES AND CO -ORDINATION....41

Key Findings and Recommended Actions....41
Immediate Outcome 1 (Risk, Policy and Coordination)....42

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES....49

Key Findings and Recommended Actions....49
Immediate Outcome 6 (Financial Intelligence ML/TF)....52
Immediate Outcome 7 (ML Investigation and Prosecution)....69
Immediate Outcome 8 (Confiscation)....79

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION....89

Key Findings and Recommended Actions....89
Immediate Outcome 9 (TF Investigation and Prosecution)....92
Immediate Outcome 10 (TF Preventive Measures and Financial Sanctions)....100
Immediate Outcome 11 (PF Financial Sanctions)....107

CHAPTER 5. PREVENTIVE MEASURES....113

Key Findings and Recommended Actions....113
Immediate Outcome 4 (Preventive Measures)....114

CHAPTER 6. SUPERVISION....131

Key Findings and Recommended Actions....131
Immediate Outcome 3 (Supervision)....133

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS....155

Key Findings and Recommended Actions....155
Immediate Outcome 5 (Legal Persons and Arrangements)....156

CHAPTER 8. INTERNATIONAL CO -OPERATION....165

Key Findings and Recommended Actions....165
Immediate Outcome 2 (International Co-operation)....166

TECHNICAL COMPLIANCE ANNEX....181

Recommendation 1 Assessing Risks and Applying a Risk-Based Approach....181
Recommendation 2 National Cooperation and Coordination....184
Recommendation 3 Money Laundering Offence....185
Recommendation 4 Confiscation and Provisional Measures....188
Recommendation 5 - Terrorist Financing Offence....190
Recommendation 6 - Targeted Financial Sanctions Related to Terrorism and Terrorist Financing 192
Recommendation 7 - Targeted Financial Sanctions Related to Proliferation....195
Recommendation 8 Non-Profit Organisations....197
Recommendation 9 Financial Institution Secrecy Laws....200
Recommendation 10 Customer Due Diligence....201
Recommendation 11 - Record-keeping....208
Recommendation 12 - Politically Exposed Persons....209
Recommendation 13 - Correspondent Banking....210
Recommendation 14 - Money or Value Transfer Services....212
Recommendation 15 - New Technologies....213
Recommendation 16 - Wire Transfers....213
Recommendation 17 Reliance on Third Parties....217
Recommendation 18 Internal Controls and Foreign Branches and Subsidiaries....217
Recommendation 19 - Higher-Risk Countries....219
Recommendation 20 - Reporting of Suspicious Transactions....220
Recommendation 21 - Tipping-off and Confidentiality....222

Recommendation 22 - DNFBPs: Customer Due Diligence....222
Recommendation 23 - DNFBPs: Other Measures....226
Recommendation 24 - Transparency and Beneficial Ownership of Legal Persons....227
Recommendation 25 - Transparency and Beneficial Ownership of Legal Arrangements....230
Recommendation 26 Regulation and Supervision of Financial Institutions....231
Recommendation 27 - Powers of Supervisors....237
Recommendation 28 - Regulation and Supervision of DNFBPs....238
Recommendation 29 - Financial Intelligence Units....240
Recommendation 30 - Responsibilities of Law Enforcement and Investigative Authorities....245
Recommendation 31 - Powers of Law Enforcement and Investigative Authorities....246
Recommendation 32 - Cash Couriers....247
Recommendation 33 - Statistics....250
Recommendation 34 - Guidance and Feedback....251
Recommendation 35 - Sanctions....252
Recommendation 36 - International Instruments....256
Recommendation 37 - Mutual Legal Assistance....256
Recommendation 38 - Mutual Legal Assistance: Freezing and Confiscation....258
Recommendation 39 - Extradition....260
Recommendation 40 - Other Forms of International Cooperation....261
Summary of Technical Compliance ï Key Deficiencies....267
Glossary of Acronyms....275

1. This report provides a summary of the anti-money laundering/combating the financing of terrorism (AML/CFT) measures in place in China (China)[1] as at the date of the onsite visit (July 9-27, 2018). It analyses the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations and the how the system could be strengthened.

摘要

a) China has undertaken a number of initiatives since 2002 that have contributed positively to its understanding of ML/TF risk, although some important gaps remain. Its framework for domestic AML/CFT co-operation and co-ordination is well established.

b) -centralised FIU arrangement consisting of CAMLMAC, AMLB and 36 PBC provincial branches has high potential to produce financial intelligence that supports the operational needs of competent authorities but its current functioning results in incomplete access by all parts of the FIU to all data, a fragmented analysis and disseminations, and limits the development of a holistic view. Therefore, major improvements are needed.

c) LEAs have access to and use a wide range of financial intelligence throughout the lifetime of an investigation, but financial intelligence is not driving ML investigations. When using financial intelligence, LEAs identify predicate criminal behaviours and actively investigate these. Predicate crime investigation outcomes reflect that China has capable LEAs that are skilled in the investigation of complex financial crime and associated predicate crime. Effective, proportionate, and dissuasive sanctions are available and are applied for ML.

d) China has an institutional framework in place to investigate and prosecute TF activities, in line with its understanding of TF risks and in line with its strategy to prevent TF and disrupt TF channels. Since the implementation

1 The following territories were not included as part of this assessment: Hong Kong Special Administrative Region (Hong Kong, China), Macau Special Administrative Region (Macau China) and Chinese Taipei.

of a new counterterrorism law in 2015 and related interpretations, the number of TF prosecutions and convictions has increased.

e) The implementation of TF and PF targeted financial sanctions is negatively affected by three fundamental deficiencies, related to (i) scope of coverage of the requirements and a lack of a prohibition covering all persons and entities; (ii) the types of assets and funds of designated entities that can in practice be frozen, and the type of transactions that can be prohibited, and (iii) a lack of implementation without delay for non-domestic designations. That said, the CTL and relevant PBC Notices are a good starting point for future updates to the legal system in line with revised FATF standards, and to improve effective implementation. While not covered by the FATF standards, authorities have taken measures in relation to other aspects of UNSCRs related to DPRK.

f) While FIs have a satisfactory understanding of their AML/CFT obligations, they have not developed a sufficient understanding of risks. Measures implemented to mitigate risk are generally not commensurate with different risk situations.

g) T supervisory system is almost exclusively focused on the financial sector, as there are no effective preventive or supervisory measures in respect of the DNFBP sector. The PBC has an inadequate understanding of risks overall. Although their understanding of risk impacting the financial sector is adequate, its understanding of institution-

rather than that of the authorities.

h) China handles MLA and extradition requests in accordance with the procedures and standards for approval stipulated by domestic laws, bilateral treaties and multilateral conventions, but due to a complicated decision-making structure for providing MLA or executing extradition requests, it is often a protracted process. At the same time, China can arrange an expedited procedure for urgent requests or cases. There is an effective cooperation in some areas between China and some of its neighbours, however, there is a lack of data that would establish effective implementation of ML/TF related co-operation.

Risks

2. The main proceeds-generating predicate crimes in China are illegal fundraising, fraud, trafficking in illicit drugs, corruption and bribery, tax crimes, counterfeiting of products, and illegal gambling.

3. China faces a serious threat from terrorism. From 2011 to 2016, China registered 75 terrorist incidents that killed 545 people. The main conflict area and focus for the authorities is the northwest province of Xinjiang, from where the "Eastern Turkistan Islamic Movement" (ETIM) operates, but attacks occur

throughout China. Around 60 people each year from China have participated as foreign terrorist fighters in Syria and Iraq[2].

4. With total assets of approximately RMB 252 trillion, banks dominate financial sector activity in China. Based on nature of their products/services and volume of activity, they are considered to be highly vulnerable to abuse with respect to ML/TF. China has witnessed a rapid increase in the activity of online lending entities, primarily via mobile phone platforms

5. The lack of coverage of designated non-financial businesses and professions (DNFBPs) by the AML/CFT framework is a significant vulnerability. The absence of coverage of domestic politically exposed persons (PEPs) is another significant vulnerability, which is particularly noteworthy in the context of a country where corruption is a major predicate offence and state-owned-enterprises play a dominant role in the economy.

6. A large amount of illicit proceeds flows out of China annually. As noted in the NRA, between 2014 and 2016, illicit proceeds totalling RMB 864 billion were repatriated to China from over 90 countries. China indicates that illicit proceeds also flow out of the country through underground banking operations. There are several instances in which criminals have fled the country, including suspects in corruption cases. The abuse of legal persons has also been identified as a method of laundering illicit proceeds. Such abuse is facilitated, in part, by ineffective arrangements in place for registering and retaining beneficial ownership (BO) information.

[illegible]

7. China has a good legal framework with respect to the criminalization of ML and TF, national coordination arrangements, the powers and responsibilities of law enforcement authorities and arrangements for international cooperation. There is scope for strengthening the legal framework with respect to a number of preventive measures and the coverage and supervision of DNFBPs.

8. An incomplete understanding of risk impacts negatively on the effectiveness [illegible] clude the

[2] See for example The Soufan Group Foreign Fighters Update Final 2015 (www.soufangroup.com/foreign-fighters), but also see paragraph 230 of this report for other estimates (up to 300 persons).

implementation of preventive measures by FIs, the supervision of these institutions and the investigation and prosecution of ML. Weaknesses in institutional arrangements and related practices impact negatively on the effectiveness with respect to the use of financial intelligence.

9. There are significant weaknesses in both technical compliance and effectiveness with respect to the transparency of legal persons and legal arrangements and the framework and practices related to targeted financial sanctions.

Assessment of Risks, Coordination and Policy Setting (Chapter IO 1; R.1, R.2, R.33)

10. Overall authorities in China demonstrated a strong understanding of the contents of the NRA which was finalized just prior to the on-site visit. However, given the focus of the NRA and the activity of LEAs, on predicate offences and the lack of attention to how the proceeds of crime are actually laundered, beyond those directly ved to a large extent, is hampered by such a focus. The assessment of risks of legal entities focuses on existing control measures. The TF assessment contained within the NRA is based mainly on qualitative analysis. The analysis collates information from departments involved in countering terrorism, primarily MSS, MPS and the PBC, identifying sources and channels of terrorist financing, and identifying the TF threats faced by China.

11. China has demonstrated strong co-operation and co-ordination at the politi cal and policy- -ordination and co-operation is the AMLJMC established in 2002 and comprising of 23 government departments. The AMLJMC is responsible for guiding the AML/CFT work throughout the country, formulating AML/CFT policies and strategies, and coordinating various departments in conducting AML/CFT activities.

Financial Intelligence, Money Laundering and Confiscation (Chapter IOs 6 8; R.3, R.4, R.29 32)

12. Provincial and local investigative agencies conduct the majority of ML and predicate offence PBC mirrors this de centralised approach with the following three largely independently functioning components: CAMLMAC and AMLB at the cen level and

AML units within each of the 36 PBC provincial branches. While the decentralized FIU in China has the potential to produce financial intelligence that supports the lyse and spontaneously share accurate and timely financial intelligence presents limitations. The analysis and dissemination by the various FIU components prevents the

analyse and share financial intelligence that is relevant for use by law enforcement. First, the STR reporting requirements only extend to FIs and their level of implementation is insufficient. Second, other sources of information, such as information on cross-border currency declarations and beneficial ownership information, are either limited or non- independence is potentially undermined.

13. LEAs at central, provincial, and local levels access and use financial intell igence and other information to identify and trace proceeds, and to support investigations and prosecutions of predicate offences, but do so for a limited extent for AML purposes. While LEAs recognis focus (when developing evidence and tracing criminal proceeds) is on supporting investigations and prosecutions of domestic predicate offences, as opposed to supporting stand-alone ML and TF investigations more broadly. The use of financial intelligence by LEAs leads to dismantling criminal networks but does not result in an adequate identification of ML operations.

14. The Ministry of Public Security (MPS) and subordinate Public Security Bureaus (PSB) have responsibility for ML investigations. The Economic Crime Investigation Department (ECID) is the branch of MPS and PSB who have the lead responsibility for investigating complex financial crime including ML. Within this department, there are skilled and capable investigators who have adequate investigative tools and resources to undertake their function.

15. There are three discrete ML offences in China. Persons who are proven to have knowledge of the requirement to launder or conceal proceeds of crime prior to the commission of the predicate crime are routinely prosecuted as predicate offence. Self-laundering is not criminalised. Accomplices and self-launders are convicted and sentenced in accordance with the predicate crime penalty, based on the principle that serious crimes absorb less serious crimes

mMM

Preventive Measures (Chapter 5IO.4; R.923)

19. FIs have a satisfactory understanding of their AML/CFT obligations. They generally have an insufficient understanding of ML/TF risks and apply mitigation measures that arenot commensurate with these risks. Online lending institutions have not developed an understanding of ML/TF risks or AML/CFT obligations.

20. FIs apply CDD measures ineffectively, withotable weaknesses in customer identification and verification measuresincluding for BO, and ongoing due diligence. Considering prevailing risks, FIs do not effectively apply measures for PEPs, TFS, and measures related to countries with high risk. FIs are relatively more successful in implementing measures related to record keeping, correspondent banking relationships, new technologies, and wire transfers.

21. Inconsistent practices of reporting suspicious transactions by FIs raise the

ML/TF risk (FIs are assessed in Chapter 5 as having a low level of understanding of risk). The quality of control measures is verified using about 20 criteria. Internal control information of uneven content and quality is also received from the sector FI regulators on their own observations on the effectiveness of internal controls applied to ML/TF risks. Theonline
of understanding of risk in the DNFBP sector is low, as little work has been done in this sector.

25. The AML/CFT supervisory system in China is heavily oriented to the financial

seems generally consistent with the overall risk profile of the financial sector, with an emphasis on banking which presents the highest levels of risk. The level of inspections in the banking sector is not commensurate with the level of risk. Sector supervisors are generally supportive but do not play a major role. There are inconsistencies in the approach used by sector supervisors. Low or no levels of supervision apply in the DNFBP sectors, with sector supervisors or SROs not playing an effective role in supervision.

26. AML/CFT financial penalties applied by the PBC average about RMB 41 million a year (approx. USD 6 02 million a year) based on 2017 statistics; these are not effective, dissuasive, nor proportionate given the size of the banks and other FIs in the financial sector, and the lack of initial responses to remedial measures. No AML/CFT remedial actions or sanctions have been applied to any online lending institutions or to DNFBPs.

27. The PBC has had a moderate impact on FIs compliance and risk management processes. The sector supervisors play a supportive role, but their impact is lower as they are mostly limited to the assessment of risk controls. There is no discernible impact on the online lending sector as specific AML/CFT requirements are not applicable. In the DNFBP sectors, the PBC and sector regulators have had a low to non-existent impact up to the time of the onsite. The overall impact of the PBC and s
moderate in the financial sector and low in the DNFBP sector.

Transparency of Legal Persons and Arrangements (Chapter 7; R.24-25)

28. Basic or legal information is collected and publicly available on the internet for all types of legal entities, although the information is not always accurate, and it

seems relatively easy to circumvent the registration rules (for example through straw persons). BO information of legal entities (domestic or foreign) is not (publicly) available in China. Authorities make use of available basic information, CDD information collected by FIs, and law enforcement powers. Each of these sources poses shortcomings and significant challenges, and the combination of measures at the current stage falls short of an effective system for obtaining accurate, adequate and current BO information in a timely manner. That said, authorities have already initiated plans and measures that may improve effectiveness in the future, including through a BO register at PBC.

29. There is no granular understanding of the ML/TF risks of each type of legal person, and the risk classification that has been produced for the purposes of the NRA focuses on control measures related to technical compliance. The Trust Law provides for the existence of domestic civil trusts. No measures have been taken to mitigate the misuse of domestic trusts, although the current risks of civil trusts are low due to a lack of regulation that would foster the use of these arrangements. Foreign legal arrangements (i.e foreign trusts) operate in China, such as the legal or beneficial owner of a Chinese legal company. Authorities have been able to detect foreign trusts that operate in China.

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

30. China has a legal and procedural framework for providing and seeking mutual legal assistance, which it uses in practice (including for extradition). The complicated procedure of ensuring a request is consistent with Chinese legislation, results in a very lengthy process, although this can be expedited in urgent cases. Feedback from -operation was mixed.

31. Judicial and law enforcement authorities seek international co-operation and legal assistance in a wide range of cases, mostly related to predicate offences, but very seldom to ML or TF. They use different channels in the efforts to return funds to the country. While China requests detention of terrorists and freezing/confiscation of and other international cooperation tools.

32. CAMLMAC exchanges information with foreign FIUs. In doing this, it sends requests abroad to a much lesser extent than it receives from foreign FIUs, which is not commensurate with the volumes of STRs analysed and work undertaken on

domestic LEAs inquiries. Supervisory authorities cooperate in a wide range of information exchange and other forms of cooperation with foreign counterparts.

The prioritised recommended actions for China, based on these findings, are

a) China should expand the information sources relied upon to formulate its NRA to include broader perspectives of the ML/TF threats, vulnerabilities, and risks it faces, publications on the subject as well as feedback from foreign jurisdictions. This will allow a more balanced understanding of the ML and TF risks faced by China beyond those directly linked to proceeds generating predicate offences.

b) China should review the functioning of its FIU to ensure that all information received, analysed and disseminated by all three FIU components is readily available and accessible both at the central and provincial levels. This review should include the creation of a database to unify and centralise all components of the current (standalone) databases at central and provincial levels. In addition, to ensure the operational independence of the FIU, China should remove the signature of the president of the PBC provincial branch as a condition for dissemination of information to competent authorities.

c) Reconsideration of the policy, which focuses on pursuit of those involved in predicate crime

d) Authorities should create comprehensive legal frameworks for the implementation of TF- and PF-related TFS that includes a general prohibition, extends to all assets of designated entities, and is implemented without delay, with regard to designations by the UNSC. In the interim, the PBC should update its existing Notice to address delays in freezing. The exiting legal framework for TF and the contemplated law on PF could be instrumental in this regard.

e) Shortcomings in the AML/CFT legal framework related to the coverage of online lending institutions, DNFBPs, domestic PEPs, TFS, and the criteria for reporting suspicious transactions should be addressed. Corresponding guidance should be provided as needed.

f) assessments of FIs, to ensure that these reflect actual threats and corresponding vulnerabilities exposing these institutions to risk; (ii) the effectiveness of ongoing due diligence, notably the monitoring of transactions; and (iii) the consolidated supervision of financial groups, to ensure a robust management of ML/TF risks by these groups.

g) The PBC should introduce an effective system of assessing individual entities' risks and supervising and monitoring DNFBPs (apart from trust

companies and DPMs) for compliance with AML/CFT obligations. In doing so, China should review the strategy and necessity of collaborating with

h) Authorities should ensure that competent authorities can obtain adequate,

Effectiveness Ratings (High, Substantial, Moderate, Low)

Technical Compliance Ratings (C compliant, LC largely compliant, PC partially compliant, NC non-compliant)

- assessing risk & applying risk-based approach	- national cooperation and coordination	- money laundering offence	- confiscation & provisional measures	- terrorist financing offence	- targeted financial sanctions terrorism & terrorist financing
- targeted financial sanctions- proliferation	-non-profit organisations	financial institution secrecy laws	Customer due diligence	Record keeping	Politically exposed persons
Correspondent banking	Money or value transfer services	New technologies	Wire transfers	Reliance on third parties	Internal controls and foreign branches and subsidiaries
Higher-risk countries					

This report summarizes the AML/CFT measures in place as at the date of the onsite visit. It analys
the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country and information obtained by the evaluation team during its onsite visit to the country from July 9 to 27, 2018. The team visited Beijing, Shanghai and Shenzhen during the onsite visit.

The evaluation was conducted by an assessment team led by staff of the International Monetary Fund (IMF) consisting of:

- Ian Carrington, Senior Financial Sector Expert, IMF (team leader)
- Richard Berkhout, Senior Counsel, IMF (legal expert)
- Arz El Murr, Financial Sector Expert, IMF (financial expert)
- Lia Umans, Policy Analyst, FATF Secretariat (FIU expert)
- Vladimir Nechaev, Executive Secretary, EAG (international co-operation and law enforcement expert)
- Craig Hamilton, Detective Inspector, New Zealand Police/APG (law enforcement expert)
- Office Portugal (legal expert)
- Alastair Bland, Consultant (NPO expert)
- Nicolas Choules-Burbidge, Consultant (financial expert)

The report was reviewed by Mr. Richard Walker (Guernsey), Ms. Paola Arena (Italy), Ms. Shereen Billings (United Kingdom), and Ms. Anne Wallwork (United States).

China previously underwent a FATF Mutual Evaluation in 2007, conducted according to the 2004 FATF Methodology. The mutual evaluation concluded that China was compliant with 8 Recommendations; largely compliant with 11; partially compliant

with 13; and non-compliant with 8. With respect to Core and Key Recommendations, China was rated partially compliant or non-compliant with 9 of the 16 Core and Key Recommendations. China was placed under the enhanced follow-up process immediately after the adoption of its 2007 Mutual Evaluation Report (MER). In light of the progress made, China was placed under regular follow-up in October 2008 and was removed from this status in 2012. The 2007 MER and follow-up reports are publicly available at www.fatf-gafi.org/countries/#China.

33. The People's Republic of China (China) was established in 1949. The country covers an area of approximately 9.6 million square kilometres and comprises 34 provinces, autonomous regions, and municipalities and special administrative regions (SARs). Beijing is China's capital city, and other major cities by population size include Shanghai, Tianjin, Shenzhen, Chengdu, and Guangzhou. China shares land borders, which stretch for 22800 kilometres, with 14 countries. At the end of 2017, China had a population of approximately 1.37 billion.

34. China continues to make progress with its policy of gradual economic opening-up which started in 1978. China implements a socialist market economy. While the state controls much of the economy, private enterprise continues to play an ever-increasing role.

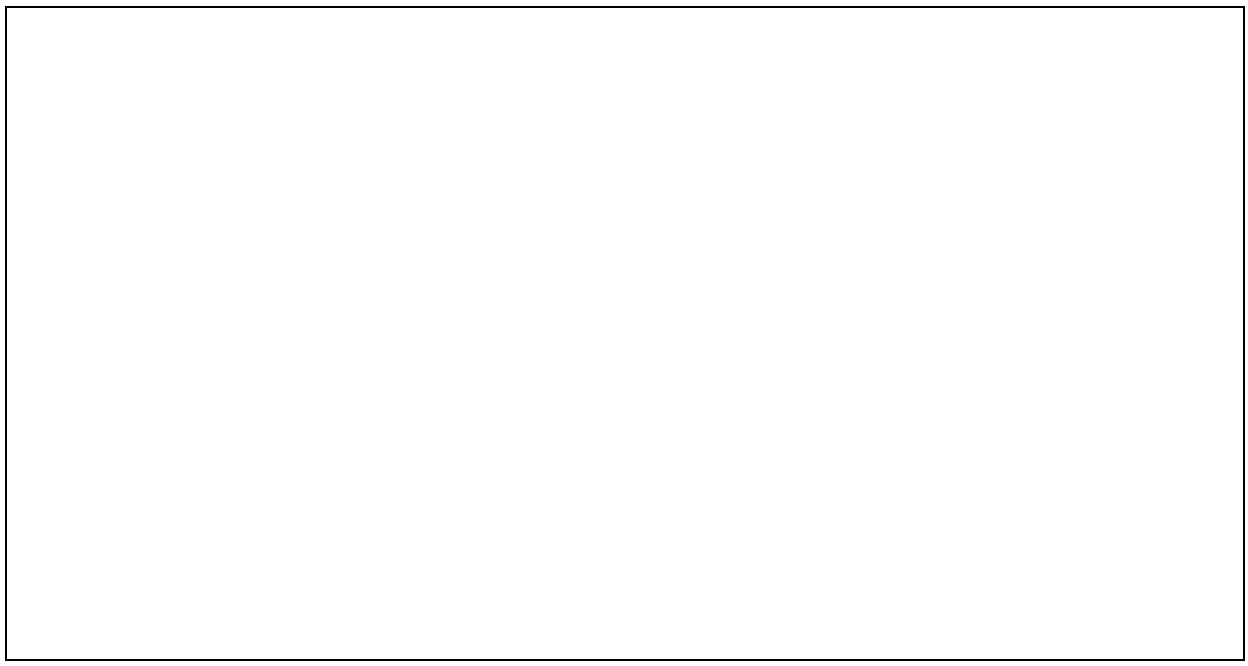
35. The National People's Congress (NPC) is the legislative branch and the highest agency of state power. It elects all supervisory, executive, judicial, and prosecutorial arms of state and has authority over local people's congresses across the country. The NPC has the power to enact and amend the Constitution and laws. The State Council is the leading body of the executive branch and reports to the NPC. It is led by the premier and has authority over all other executive state agencies. It has the authority to develop administrative legislation and regulations in accordance with the provisions of the Constitution. Departmental regulations can be issued by ministries and commissions of the State Council, the PBC, the National Audit Office, and institutions under the State Council which perform administrative functions.

36. The Supervisory branch is accountable to the People's Congress, and independently exercises supervisory power in accordance with the Constitution.

37. The judicial branch is comprised of the People's Courts and the People's Procuratorates, which exercise their powers independently from each other in accordance with the Constitution and are both subject to the supervision of the People's Congress.

38. The Constitution of China is the highest law in the country. Other laws in hierarchical order are laws, administrative regulations, local regulations, and rules.

National and local administrative regulations are administered by the ministries under the State Council and local executive agencies respectively.



Overviewof ML/TF Risks

ML/TF Threats

39. The highest ML threat in China stems from illegal f Q q 0 0 595 6( )-15.996 (f Q q 0 0 595 6(9

other jurisdictions.[4] The NRA indicates that illicit proceeds flow out of the country through underground banking operations and that between 2014 and 2016, illicit proceeds totalling RMB8 64 billion were repatriated to China from over 90 countries. China indicates that the proceeds recovered during this two-year period, are estimated to have flownout of China over a period of 20 years. The NRA highlights that there are /Ta indi. dies. ndiiod, oe atndi2ear04 (i)-4.00fle (2)-1100d02 7h

etween.ri.ee

currently undertaking comprehensive actions to clean up the sector. However, the sector is not subject to ongoing AML/CFT supervision by the PBC. The NRA highlights that at the end of 2016, transaction volumes of RMB 2 trillion and loans outstanding of RMB 816.2 billion in this sector had grown by 110% and 101% respectively, over the previous year. It also indicates that non-bank payment sector has experienced rapid growth with transaction volumes escalating from RMB 17.6 trillion to approximately RMB 100 trillion from 2013 to 2016. While mobile payments must be linked to a commercial bank account and, as of end-June 2018, channeled through a central clearing house, the non-face-to-face feature of mobile payments, as well as the use of bearer prepaid cards represents a notable level of ML/TF vulnerability. Private sector entities have reportedly also been engaged in business with entities from higher risk areas, such as those countries targeted as high risk by FATF or those countries with entities that are subject to UN-based targeted financial sanctions (TFS).

43. China does not have effective arrangements in place for registering and retaining beneficial ownership (BO) information. The lack of coverage of designated non-financial businesses and professions (DNFBPs) by the AML/CFT framework is a significant vulnerability, especially considering the sustained growth in the real estate and precious metals sector and opportunities for legal professionals to exploit weaknesses that can facilitate the abuse of legal persons. The absence of coverage of domestic politically exposed persons (PEPs) is another significant vulnerability, which is particularly noteworthy in the context of a country where corruption is a major predicate offence and state-owned-enterprises play a dominant role in the economy.

Underground Banking

44. China has a large underground financial sector with broad international connections. It consists of unlicensed operatives who provide financial services including, payments, settlements, remittances and currency exchange. The NRA indicates that this sector, which is considered to facilitate the movement of significant amount of illicit proceeds, provides a wide range of services, including remittances, overseas cash withdrawals with bank cards, foreign exchange, and point-of-service (POS) machine cash. Although competent authorities believe that underground banks do not have a direct link to the formal financial system, they recognise that underground banks may illegally utilise the settlement network of financial

institutions (FIs) to conduct activities. The competent authorities consider that the trend for using underground banking in TF is on the rise and both law enforcement agencies (LEAs) and financial sector supervisors are concerned about this development.

45. The NRA indicates that in 2015, LEAs cracked down at least 170 major cases and in 2016, national public security agencies also resolved 380 major cases of underground banking, arrested 800 suspects, and closed 500 locations where the activity took place. It also indicated that in 2017, a total number of 468 major underground banks and ML cases have been resolved with 892 criminal suspects arrested and 1100 operating centres destroyed. Notwithstanding these initiatives, the authorities still consider underground banking to be a thriving activity.

Fintech Products

46. China has witnessed a rapid growth in the use of Fintech products, particularly in the non-bank payment sector (see below section on Financial sector and DNFBPs). According to the NRA, there were approximately 164 billion internet payment transactions conducted in this sector in 2016, representing an almost 100% increase from the previous year. Many institutions that operate in this sector are increasingly offering products that facilitate cross-border transactions. The authorities' concerns about the ML/TF vulnerability of these products relate to the ease with which accounts can be opened and the non-face-to-face nature of the delivery channel. While limits are set for individual transactions, the authorities are concerned that criminals could use multiple accounts for ML/TF purposes.

47. Since 2017, the PBC has started to work with sector regulators and other government agencies to develop measures to address risk associated with the rapidly developing internet financial activity. Current initiatives are expected to lead to the development of a Fintech regulatory framework including guidance to be issued to the industry.[17]

7 80.

1

‘ — • – ”R ï • [illegible]

‘ — • – ” › ïk•Assessment

48. China completed its first NRA in 2017. It draws primarily upon an analysis of 680 000 published court judgements from 2013 to 2015 to inform itself of threats to the country's economy and social order. The NRA also analyses inherent risks and the mitigating controls in place related to financial sector products and the activities of some DNFBPs. The NRA analyses the various proceeds-generating crimes in China both on a national and regional basis. It identifies illegal fundraising, corruption, telecommunications and internet deception fraud, and drug trafficking as the four major proceeds-generating crimes accounting for more than 70% of the estimated criminal proceeds generated in China.

49. The NRA identifies the ETIM as the main TF threat to China with limited

quantitative data and qualitative data (including cases), and information obtained through interviews with counter terrorism departments.

Scoping of Higher-Risk Issues

50. Assessors focused on how cases involving proceeds from the main predicate offences are investigated and prosecuted and proceeds are confiscated. They assessed the use of financial intelligence with respect to both ML and TF cases.

51. Considering their dominance of financial sector activity and the nature of their products and services, the team assessed banks' understanding of ML/TF risk, the risk management systems in place, and the challenges, if any, that the strong presence of state-owned banks present for effective supervision.

52. Considering the significance of cross-border transfers and the volume of criminal proceeds that flow from China to several international destinations, attention was paid to the activity of the non-bank money or value transfer services sector. Due to the rapid growth of their activities, assessors paid attention to the online lending and payment sectors. The assessors' attention also focused on the supervision of the above categories of FIs, as well as the fast-growing Fintech sector.

53. Due to the deficiencies in the transparency of beneficial ownership of and the documented abuse of legal persons, assessors focused on China's ability to trace funds

and ownership information through corporate structures and, in general, the effectiveness of arrangements in place to prevent abuse of these structures.

54. Considering the substantial volume of illicit proceeds flowing out of China and the incidence of suspects fleeing the country, assessors examined the measures in place with respectto international cooperation generally, as well as the effectiveness of border protection and customs agencies.

55. The team assessed law enforcement's and prosecution's understanding of the TF risk and TF investigations and prosecutions, including the use of financial intelligence, both domestically and in cooperation with foreign counterparts.

obligations related to TFS.

Areas of Lesser Risk and Attention

56. Group financing companies and asset management companies whose activities are focused primarily on managing portfolios of nonperforming loans of domestic FIs have a lower level of ML/TF risk as they are limited with respect to the volume of their transactions and interaction with third parties. The assessment team devoted lesser attention to these areas.

Overview

57. China's GDP grew by 6.8% in 2017 with nominal GDP reaching RMB82.1 trillion. The average annual GDP growth rate over the five-year period from 2013 to 2017 was7.1%, and the unemployed rate has averaged 5.1% over the period. China is transitioning from high-speed to high-quality growth, and the authorities have set a GDP growth target of 6.5% for 2018.[8] Domestic credit to the private sector, which averaged 15% over the 5-year period, fell to 12.8% in 2017.[9]

58. China has a large and complex financial sector. 18 main commercial banks (including 5 large commercial banks, 10 joint-stock commercial banks and 3 policy/development banks) account for 69% of the total assets of the banking sector. Banks dominated financial sector activity with total assets of RMB252 trillion at the end of 2017. China's banking sector has witnessed rapid

8 IMF, China Article IV Report, p. 59.

9 IMF, China Selected Indicators, China Article IV Report 2018, p. 3.

growth over several years. This trend has moderated over the past year and growth in banking sector assets of 8% in 2017 was half the rate of growth for the previous year, and banking sector assets fell as a percentage of GDP for the first time since 2011.[10] Assets of insurance and capital market institutions totalled RMB 16 and 13 trillion respectively.

Overall Level of Compliance and Effectiveness

59. China has a stable political system and well-developed institutional infrastructure. The Anti-Money Laundering Joint Ministerial Conference (AMLJMC), comprised of 23 different government departments, has been meeting regularly since 2002 to direct and co-ordinate the implementation of the AML/CFT framework, with the State Council approving the outcomes of its work.

Assessment of Risk, Coordination and Policy Setting

60. There are strong and mature institutions across the public sector and mechanisms are in place for the national co-ordination of AML/CFT initiatives. Regulatory objectives and strategies are transmitted through a multiplicity of secondary legal instruments with a degree of duplication in several instances, which has the potentia
size requires a fragmentation of the institutional arrangements which presents coordination challenges, some of which were observed by the assessment team.

61. Corruption is considered to be a significant predicate offence, and the authorities have prioritised anti-corruption initiatives. There is, however, no strong indication in terms of the operation of government agencies, that corruption has negatively impacted the overall effectiveness of the AML/CFT system.

AML/CFTStrategy

62. the Opinion on Strengthening the Supervisory Framework and Mechanism for Anti-Money Laundering, Countering the Financing of Terrorism and Anti-Tax Evasion (State Council GAD Letter No. [2017] 84) issued by the General Office of the State Council. The strategy emphasizes the role of the AMLJMC as the national coordination body and the PBC as the leading AML/CFT

10 IMF, China Article IV Report, p. 8.

authority. Its objectives include strengthening the legal and regulatory framework, the capacity of AML/CFT institutions and cooperation among the agencies. The strategy also seeks to strengthen international cooperation.

Legal and Institutional Framework

Policy Coordination Bodies

63. The AMLJMC is the highest AML/CFT coordination body in China. It is led by the Governor of the PBC, and its membership includes the main AML/CFT government agencies.

64. The ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ^(PBS) is the central bank and the principle AML/CFT authority in China with responsibility for co-ordinating all national initiatives. It houses the Anti-Money Laundering Bureau (AMLB) and the China Anti-Money Laundering Monitoring and Analysis Centre (CAMLMAC). The PBC, in collaboration with sector supervisors, is the main AML/CFT supervisor of FIs.

65. The PBC hosts the Financial Intelligence Unit (FIU) which consists of CAMLMAC, the AMLB and the 36 PBC branches, each of which executes aspects of the components together as Š ‹ • ƒ ï • ƒ ” ” ƒ . • ‰ ‡ • ‡ • –

66. CAMLMAC and all of the information contained in key STRs directly reported to the 36 PBC branches at provincial level. It undertakes analysis, makes disseminations to central LEAs or forwards information to the AMLB or provincial branches for administrative investigations.

67. The AMLB is responsible for supervision, administrative investigations, policy oversight, and the overall coordination of the PBC

70. The SPPsupervises and directs arrests and prosecutions with3 ( )-93.995 (and)2.998 (98 -Ft2

79. The China Securities Regulatory Commission (CSRC) is the prudential regulator for securities institutions and supports the PBC on AML/CFT supervision.

80. The State Administration for Foreign Exchange (SAFE) is administratively part of the PBC and is in charge of supervising foreign exchange transactions.

81. The Ministry of Justice (MOJ) coordinates mutual legal assistance (MLA) pursuant to relevant treaties and conventions. It is also responsible for licensing and supervising lawyers and notaries.

82. The Ministry of Finance (MOF) is responsible for licensing and supervising accounting firms, and certified public accountants. It is also responsible for allocating budget to competent authorities, including to the PBC and its branches.

83. The Ministry of Foreign Affairs (MFA) develops policies on international co-operation with other governments and leads on the implementation of UNSCRs. It coordinates regional AML/CFT organisations.

84. The Ministry of Housing and Urban-Rural Development (MOHURD) is responsible for the supervision of the real estate sector.

85. The Shanghai Gold Exchange (SGE) is a non-profit self-regulatory body established by the PBC. It supervises large-scale gold trading conducted by its members who consist of persons authorised to trade in gold in China. The members include major gold producers, processors, and retailers, but does not cover the downstream network of 11 500 institutional customers.

Financial Sector and DNFBPs

Financial institutions

86. Banks dominate financial sector activity in China. As of December 31, 2017, assets of commercial banks (large commercial banks, joint stock commercial banks and urban commercial banks) and the assets of rural banks and other deposit-taking institutions totalled RMB 252 trillion.

87. The activity of foreign branches and majority-owned subsidiaries is significant - owned subsidiaries are owned by the top five banks. As of the end of 2017, these banks had 1270 overseas branches, accounting for 1.85% of the total number of

branches (68 for 12% of the total assets (RMB 92.82 trillion) of the top five banks

88. There are licensed capital market entities in China with assets totaling RMB 13.5
activity. Assets held by insurance entities totaled RMB 16.8 trillion.

11					
		2			
		2			

11 Can only be operated within one county. Total assets account for 13% of the total for the banking sector.

1

		2			

89. Online lending is one of the 7 categories[12] refers to direct lending between individuals through internet platforms (also referred to as "P2Ponline lending"). These platforms provide intermediary services, including information exchange, matching, and credit rating assessment, for investors and financiers, as well as credit loans directly from microlending companies to users. Most P2P credit loans are processed through internet platforms, while P2P collateral loans require offline review. Currently, personal loan amounts do not usually exceed RMB 200 000. Corporate loans cannot exceed RMB 1 million. Accumulated loan amounts across allonline lending platforms cannot exceed RMB 1 million for natural persons

DNFBPs

The following DNFBPs operate in China but have not be designated under the AML Law:

- : At the end of 2017, there were approximately 130 000 real estate agencies in China, employing over one million agents. The sector is estimated to generate income in excess of RMB 15 billion annually.
- d its network of institutional customers. No data have been provided on the number of persons who trade with SGE members or the number of unorganized/unregulated DPMs outside the SGE framework.
- in China must be part of a law firm. It is estimated there were 325 500 lawyers in China at the end of 2016 and 28 800 law firms.
- At the end of 2016, there were 13 175 notaries in China and 3 001 notary institutions. Notaries dealt with 13 990 000 cases during 2016.
- At the end of 2016, there were 105 200 certified public accountants in China and 7 408 accounting firms.
- No data have been provided on the number of such providers.

92. It is illegal to operate casinos in China.

93. When assessing the effectiveness of preventive measures and AML/CFT supervision, the assessment team gave the highest importance to banks, followed by payments institutions. The securities and futures, insurance, internet finance, real estate agents, company service providers, and DPM were considered to be at a medium level of importance. Less importance was given to other DNFBPs sectors.

Preventive Measures

94. -out in the AML Law and a vast number of secondary legal instruments, including regulations, notices, administrative measures, opinions, rules, and guidelines. In the process of conducting the assessment, the team reviewed more than 30 AML/CFT regulations in addition to many other secondary legal instruments relevant to the assessment. This fragmented framework results in several instances of overlap and duplication across the legal

framework and, in some cases, makes it difficult to understand the source and nature of specific obligations.

Legal Persons and Arrangements

Legal Persons

95. There are three types of legal persons in China: (i) special public legal persons; (ii) non-profit; and (iii) for-profit legal persons:

i. Special legal persons include state agency legal persons (2 300), basic self-governing mass organizations (660 000), rural collective economic organizations (7 700), and urban and rural cooperative economic organizations (2 017 000). These legal persons are created by state organisations. The latter can undertake commercial activities, and although the ownership of these entities is collective, the control is not. These types of legal persons are for the most part not covered in this report.

ii. Non-profit legal persons include public institutions (970 000), social groups (352 000), foundations (6 300), social service organizations (397 000), and overseas NGOs (393). These entities are covered under IO.10 (NPOs).

iii. For-profit legal persons consist of limited liability companies (LLC, 23 798 000), joint-stock limited companies (JSLC, 140 200), state-owned enterprises (357 000), listed companies (3 400), and foreign investment enterprises (539 000). These foreign investment enterprises include wholly owned foreign enterprises, Chinese-foreign equity joint ventures, and Chinese-foreign contractual joint ventures. Other for-profit legal persons include enterprises owned by the whole people, enterprises owned collectively, private enterprises, and associated enterprises. In addition to these, there are also legal entities that do not qualify as legal persons under Chinese law, but that are nonetheless relevant for this report. These other for-profit quasi-legal persons include other non-corporate persons that do not meet the requirements of legal persons, partnerships (556 000), sole proprietorships (2 586 000), enterprises of foreign jurisdictions that are involved in business operations within China, resident and representation offices of foreign enterprises. LLCs and JSLCs are also referred to as on the terms used in the Company Law.

96. Notably, the Civil Law defines for-profit legal

without indicating what these other for-profit legal persons are. This provides legal flexibility as China continues its reforms, but also creates some uncertainty as to the types of legal entities that exist.

Legal Arrangements

97. In addition to foreign trusts, which are not recognised or regulated in China but can undertake business in China (e.g., owning Chinese companies), the Trust Law recognises three types of trust: (i) civil trusts; (ii) charitable trusts; and (iii) business trusts. In the previous FATF/EAG assessment report of China, all of these trusts were considered to meet the definition of legal arrangements under the old R.34; however, under the current standard only civil trusts meet the definition of legal arrangement.

- There are three types of civil trusts: wealth, educational, and testamentary. Educational civil trusts aim to provide funds for education; testamentary civil trusts aim to ensure that the will of a deceased is executed (as far as the distribution of assets of the deceased is concerned); and wealth civil trusts allow a person's wealth to be managed by another person. Unlike business trusts and charitable trusts, civil trusts are not regulated by the CBIRC and the only legal provisions governing civil trusts are those found in the Trust Act. While the legal framework explicitly requires business and charitable trusts to be managed by trust companies, no professional trustees are required for civil trusts. As was indicated in the previous assessment report, it remains possible for civil trusts to be established and administered outside the regulated sector. According to authorities and (academic) literature, civil trusts are said to be rarely used in China, which is in line with the observations of the assessment team.
- The assessment team considers that business trusts despite their name do not meet the FATF definition of legal arrangements, but that these are financial investment products offered by trust companies that are financial institutions (as covered under IO.3/IO.4 in this report).[13]

13

100. China does not have one central authority dealing with MLA requests. It has established a mult-channel method of carrying out international cooperation. Government agencies which are involved in this process include the MOJ, the MPS, the MFA, and the SPP[14].

14 The function has been transferred from the SPP to the NSC.

Key Findings

a) Since 2002, China has demonstrated an ongoing practice of developing AML/CFT policies and risk mitigation activities based on risk assessments, as evidenced by the number of threat, vulnerability, and risk studies conducted in China since that time, and the subsequent issuance of opinions, measures, regulations, and laws resulting from such studies. With the publication of its first NRA in June 2018, China has formalized the process for identifying and assessing its ML and TF risks.

b) coordination is well established. The AMLJMC, comprised of 23 different government

importance the authorities attach to AML/CFT. The PBC is the lead department responsible for formulating and updating the AML/CFT strategy which is published by the State Council and to which implicated departments are held accountable through the national audit process.

c) While China demonstrated that it has a good understanding of ML/TF risks and that its understanding of risk was not based solely on the NRA but rather on its long history and practice of undertaking threat, vulnerability and risk assessments, its understanding has gaps. Notable among them are DNFBPs (expanded upon further in the following Key Finding) and legal

risks is hampered, to some extent, by an overreliance on known threats derived from the analysis of predicate offences thereby missing information on the methods and trends of ML activity that would only be derived from ML crimes that were not prosecuted.

d) While there is a reasonably good understanding of risks at the sectoral level for DNFBPs, there is a lack of risk assessments of individual DNFBPs due to the absence of supervisory arrangements. China is aware that the lack of guidance for DNFBPs represents a vulnerability along with the failure of understanding of ML/TF risks faced by DNFBPs would be significantly enhanced once AML/CFT obligations are fully and properly imposed on all entities in the DNFBP sectors.

2

Recommended Actions

a) China should expand the information sources relied upon to formulate its NRA to include broader perspectives of the ML/TF threats, vulnerabilities, publications on the subject as well as feedback from foreign jurisdictions. This will allow a more balanced understanding of the ML and TF risks faced by China beyond those directly linked to proceeds generating predicate offences.

101. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are Rs.1, 2, 33, and 34.

Understanding of its ML/TF Risks

102. China has demonstrated a pattern of studying threats, vulnerabilities and risks on a variety of subjects related to ML since the inception of AMLJMC in 2002. With the completion and subsequent publication of its first NRA in June 2018, China has formalized the process for identifying and assessing its ML and TF risks. The NRA is a culmination of a two-year effort that involved input from 23 government departments as well as different FIs and DNFBPs.

103. While considering a range of credible information sources primarily draws upon an analysis of 680000 published court judgements of predicate offence economy and social order. The NRA places, however, a focus on predicate offences and lacks sufficient attention to how the proceeds of crime are actually laundered beyond those directly implicated in the predicate offence. While authorities in China demonstrated a strong understanding of the contents of the NRA and proceeds genera to be much lower.

104. The NRA also analyses inherent vulnerabilities and the mitigating controls in place related to financial sector products and the activities of some DNFBPs. The NRA preventive measures, such as the system of laws and regulations, supervision, and the effectiveness and/or weakness of criminal penalties, law enforcement mechanisms

and capabilities. For example, in discussing supervision relative to CFT, the NRA

working systems. First, the specific coverage of DNFBPs in China is not clear. China has not yet specified the AML/CFT obligated DNFBPs, which is mentioned the in laws and regulations. Second, the detailed CFT obligation requirements for DNFBPs have not been issued. At present, there are no detailed requirements specific to DNFBPs on customer identification, due diligence, or transaction reporting. Overall, there is a lack

indicated that these gaps were identified at the beginning of the NRA process in early 2017, at the time of the onsite visit, authorities were unable to demonstrate an understanding of the ML/TF risk faced by most DNFBPs.

105.
threats, as evaluated by an analysis of adjudicated criminal cases of predicate offences, thereby missing information on specific methods and trends of ML activity that were not prosecuted
position that their Criminal Law does not allow the prosecution of self-laundering in addition to the prosecution of a predicate offence, and their position that most ML crimes are committed by the predicate offenders themselves. The self-laundering activity becomes an aggravating factor in sentencing of the predicate offence. China asserts that the investigation and prosecution of ML activity is generally inseparable from the predicate offence. For example, China identified illegal fundraising as the highest proceeds generating crime, yet ML prosecutions where illegal fundraising is identified as the predicate offence, represents less than 1% of the ML convictions.

106. ETIM as the main TF

addresses some fundraising techniques, mainly self-funding through the sale of personal assets and family support. The TF assessment contained within the NRA is based mainly on qualitative analysis. The analysis collates information from departments involved in countering terrorism, primarily MSS, MPS and the PBC, identifying sources and channels of terrorist financing, and identifying the TF threats

and law enforcement CFT work, and analyses the vulnerabilities. In reference to DNFBPs however, as stated earlier, the NRA notes a lack of coverage of DNFBPs and concludes that there is a lack of relevant regulation and guidance for CFT measures in DNFBPs.

107. While China has addressed risk for some DNFBPs in the NRA, the PBC has not conducted any risk assessment of individual DNFBPs (aside from trust companies) thereby missing information related to risks posed by the clients of DNFBPs and their products that would have been available were the sectors appropriately supervised for AML/CFT. The CSP and DPS sectors are not discussed in the NRA and are unrated. During the onsite visit, the DNFBP sector supervisors (the MOHURD, the MOF, and the MOJ) demonstrated a low level of understanding of ML/TF risk within their supervised sectors. The authorities stated that the sector supervisors are actively involved in the ML/TF risk assessment process, but no specific or detailed information was provided to demonstrate this.

108. While an important step in contains some gaps in its analysis of ML/TF vulnerabilities. One such example was identified in the context of FIs conducting customer due diligence (CDD) measures. channel to inquire about the BO information of legal persons and legal arrangements. Most banks do not carry out

address company service providers (CSPs).

109. Another example of gaps in the NRA relates to the assessment methodology: the risk mitigation factors considered are, in some instances (e.g., in the vulnerability assessment of the real estate sector) not the controls specified in the AML Law, rather the NRA considers various sector controls either unrelated to, or only indirectly related to, AML/CFT controls.

110. Chinese authorities indicated that the NRA was a confirmation of a pre-existing understanding of ML/TF risk formulated over the past several years from the various industry risk assessments conducted and the Annual National Threat Assessment exercise. of understanding of risks, supported by the long-standing practice of threat, vulnerability, and risk studies conducted in China, and the subsequent co-ordinated actions to combat predicate offenses ML and TF.

National Policies to Address Identified ML/TF Risks

111. As mentioned earlier, China has demonstrated a pattern of studying threats, vulnerabilities and risks on a variety of subjects related to ML since the inception of AMLJMC in 2002. These studies, as is the case with the NRA, resulted in action plans

often involving the issuance of opinions, measures, regulations and laws to serve as mitigating factors to address the risks identified. Through the oversight of the State Council, and the national audit process, implicated departments are held accountable to delivering on these action plans

112. In 2013, China established the National Leading Group for Countering Terrorism (the Leading Group). The Leading Group plays a leading role in intelligence warning, prevention, emergency response, aftercare, and publicity in every aspect of countering terrorism, including terrorism financing. The Leading Group is served by State Councillors, which consists of a leading group office and a countering terrorism operations office. The members of the Leading Group include fixed members and ad hoc members. The fixed members include the MFA, MPS, MSS, and the PBC, while ad hoc members may include the Ministry of Transport, Ministry of Civil Affairs, Ministry of Health, etc. depending on the topics to be discussed/addressed. The Leading Group sets policies and drafts action plans, the latest of which was shared with the assessment team but for security reasons are not published publicly. After the establishment of the Leading Group, various provinces, autonomous regions, and cities also established local leading groups accordingly.

Exemptions, Enhanced and Simplified Measures

113. China identified bank cards as high-risk products. In response, China points to the Notice of the PBC on Strengthening the Administration of Bank Card Business (PBC Document No. [2014] 5) and the Notice on Further Strengthening the Anti-Money Laundering Work of Bank Card Business (PBC GAD Document No. [2014] 124) as two examples of enhanced measures put in place to mitigate the risk related to bank cards. These notices strengthened requirements for the identification during the application and usage of bank cards outlined in the AML Law and the Administrative Measures for Customers Identification and Documentation of Customers Identity Information and Transaction Records by Financial Institutions

114. China indicated that FIs are permitted to implement certain simplified measures. Jointly with regulatory authorities, FIs are to evaluate the ML/TF risks of the relevant business products, including the vulnerabilities of adopting any recommended simplified measures. Any simplified measures adopted must be done through reaching a mutual agreement with the regulatory authorities. One such example was in 2016 when, after assessing the risk of various account activity, the

PBC issued a classification system for personal bank accounts. Accounts were classified into three categories: I, II, and III. Category I is an unrestricted, fully functioning bank account that must be opened in person at the FI and is subject to on-site verification of identity. Only one Category I account is permitted per customer per FI. Category II accounts allow for the electronic transfer of funds, the purchase of financial products, and for making payments of less than RMB 10,000 per day. Category II accounts are restricted however, and cannot be used to withdraw cash. Category III accounts only allow for small value consumption and payments with the account balance of no more than RMB 1,000. Based on an identification of low ML risk and in an effort to enhance convenience and inclusiveness of financial services, China allows Category II and Category III accounts to be opened through banking, mobile banking, and other electronic channels without providing identity information repeatedly or showing identity documents, thus simplifying control measures. China indicated that no risk incidents have arisen from adopting these simplified measures.

Objectives and Activities of Competent Authorities

115. The prevalence of underground banking has been identified by China as a risk related to ML/TF in that it provides a vehicle for the remittance of illicit income to foreign jurisdictions with ease. In response to this risk (see IO.7) MPS has focused resources and efforts on this criminal behavior with considerable success. Authorities report that in response to these efforts they are seeing a reduction in the prevalence of underground banking.

116. CAMLMAC prioritises its strategic analysis initiatives to focus on financial transactions associated to predicate crimes, which are identified as higher risk through the NRA and other assessments. These initiatives resulted in various high-risk crime related typologies reports disseminated to LEAs to assist them in prioritizing their financial investigations. LEAs advised that these strategic analysis products are very helpful and assist them in setting priorities for their investigations. It should be noted however, as outlined in detail in both IO.6 and IO.7, LEAs use financial intelligence primarily to drive predicate investigations, as opposed to ML investigations. In addition, as identified in the write up IO.6, the majority of criminal investigations using financial intelligence from CAMLMAC originate in requests from LEAs rather than spontaneous disseminations by CAMLMAC.

National Coordination and Cooperation

117.

are limited to the financial activity associated to the proceeds of a specific criminal act as opposed to comprehensive financial investigations related to criminal activity more generally. It is analogous to pursuing the proceeds of a drug transaction as opposed to pursuing the assets of a drug trafficker.

121. While China lacks a comprehensive legal framework to deal with targeted financial sanctions related to proliferation financing (see IO.11), the MFA and the PBC have coordinated on steps to implement UNSCR requirements for the financial sector. The MFA is responsible for informing other state entities of the existence of new UNSCRs related to PF. PBC is then responsible for communicating the UNSCRs (based on PBC Notice 187/2017) as well as issuing risk warnings to selected vetted FIs. As far as domestic coordination is concerned, to support implementation by banks, the PBC has provided training and asked selected banks to screen their entire database against the UNSCRs. Furthermore, as detailed in IO.11, the authorities have coordinated to implement measures against PF, such as in relations to export control measures and the smuggling of banned goods.

Private ‡ … –Awäreness of Risks

122. Many private sector entities were involved in the development of the NRA alongside government entities. Electronic copies of the NRA were sent to government departments and the major financial institutions. Smaller FIs and other regulated entities were provided copies through their local PBC branches. The NRA was also distributed to industry association bodies where it is available to DNFBPs. The distribution method used for the NRA has also been used to distribute the Annual National Threat Assessments with a summary version posted on the PBC website.

123. While the NRA was only published in June 2018, as identified earlier, China has produced, and shared numerous threats, vulnerability, and risk studies related to specific topics over the past several years. In addition, CAMLMAC produces strategic analysis products and ML/TF risk reminders to guide FIs in their identification of ML/TF risks and facilitate and increase the quality of STR reporting. In addition to CAMLMAC, local PBC branches will issue guidance and risk warnings as well.

Overall Conclusions

Key Findings

Immediate Outcome 6

a) LEAs have access to and actively use a wide range of financial intelligence throughout the lifetime of an investigation to identify and trace proceeds. However, their focus is mainly on supporting investigations of domestic predicate offences, and to a lesser extent on supporting ML and TF investigations and developing ML and TF evidence.

b) centralised FIU arrangement consisting of CAMLMAC, AMLB and 36 PBC provincial branches has high potential to produce financial intelligence that supports the operational needs of competent authorities but its current functioning results in incomplete access of all parts of the FIU to all data, fragmented analysis and disseminations, and limits the development of a holisticor integrated or comprehensiveview to financial intelligence.

c) analyse and share financial intelligence that is relevant for use by law enforcement. First, the STR reporting requirements only extend to FIs and their level of implementation is insufficient. Second,other sources of information, such

successfully prosecute ML. Most ML prosecutions involve immediate family members and close associates of predicate offenders, which confirms that a limited impact on the effectiveness of ML investigations and prosecutions There have been three occasions where legal persons have been charged with ML.

c) Predicate crime investigation outcomes reflect that China has capable LEAs that are skilled in the investigation of complex financial crime and associated predicate crime. Financial intelligence is not routinely driving ML investigations. It is however, identifying predicate criminal behaviours which are actively investigated.

d) Effective, proportionate, and dissuasive sanctions are available and are applied for ML. In addition, there exists a range of alternative measures which can be applied when prosecution for ML is not possible or not appropriate. These include administrative sanctions, administrative forfeitures, and the use of disciplinary procedures which can be imposed by the CCP against its membership.

Immediate Outcome 8

a) China demonstrates a commitment to deprive criminals of property through the seizure and confiscation of instruments of crime and criminal although the accuracy of statistics collection and analysis to monitor and improve performance could be improved and an extension of the non-conviction framework or a broadening of the unexplained wealth provisions could be considered.

b) The NRA acknowledges that substantial amounts of criminal proceeds flow from China to foreign jurisdictions through underground banks. In recognising this weakness, considerable effort has been invested to target and dismantle underground banking networks. This is commendable. Authorities report that they are detecting less such activity as a result of their enforcement efforts; however, the activity persists and continues to provide for a mechanism to remit the proceeds of crime to other jurisdictions. Focus of recovery of foreign remitted illicit proceeds that has exited China is a current policy objective which has resulted in the recovery of significant amounts of proceeds of crime.

c) China borders 14 countries and experiences hundreds of millions of movements of people and goods, therefore challenges are significant. A currency declaration system operates in China and enforcement occurs with focus on people, and to a lesser extent mail and cargo. Resources and equipment are deployed to high-risk border crossing entry and exit points which have a degree of effectiveness, further investment of resource is occurring at other entry and exits points, mail centres and at ports. China acknowledges its border risk and the need to implement processes to

improve the flow of information and intelligence between the border agency, the PBC,[15] and the neighbouring jurisdictions.

Recommended Actions

Immediate Outcome 6

a) In addition to the current use of financial intelligence for predicate offence investigations, LEAs should also focus on using this intelligence to initiate and conduct ML and TF investigations and tracing related assets, and to develop ML and TF evidence.

b) China should review the current functioning of its FIU to ensure that all information which is received, analysed and disseminated is readily available and accessible to all constituent parts of the FIU at both the central and regional levels. This review should include the set up of a database to unify and centralise all components of the current (stand-alone) databases at central and provincial levels.

c) To ensure the operational independence of the FIU, China should remove the requirement for the signature of the president of the PBC provincial branch as a condition for dissemination of information to LEAs and other competent authorities. CAMLMAC and the provincial branches should include financial intelligence from counterpart FIUs in their standard practices for analysis and dissemination of information.

Immediate Outcome 7

a) A review of the current legislation and consolidation of the ML offence and the receiving offence into two separate and distinct single articles is necessary.

b) Authorities should remove the threshold for the criminalisation of ML (Art. 312) and in addition amend

; or similar wording as appropriate under Chinese law) and increase the understanding and use of the ML offense by the prosecution and judiciary in practice. This would enable the ML offence to be applied against a much wider range of ML behaviours.

c) The authorities should reconsider the policy, which focuses on pursuit of those involved in predicate crime to include one that has a broader focus

predicate crime, which will identify more persons (natural and legal) undertaking ML activities.

d) China identifies significant risks with underground banking, and therefore the strategy should extend beyond the current disruption activities to that of a focus on the identification of third-party launderers and predicate offenders who are using the services of underground bankers to launder

[15] NRA, p. 221.

chosen this approach. However, the assessment team has serious concerns regarding the implementation of this decentralised approach in China, as set out in detail below.

- x CAMLMAC;
- x The AMLB; and
- x Anti-Money Laundering Units within each of the 36 PBC provincial branches.

128. CAMLMAC is established at the central level and has primarily responsibility for the receipt and analysis of large-value transaction reports (LVTRs) and ordinary suspicious transaction reports (STRs) (i.e., transactions related to criminal activities such as ML, TF, and predicate offences as STRs). CAMLMAC also receives the information contained in all key STRs directly and simultaneously reported to the 36 provincial PBC branches. It thus centralises the receipt of disclosures filed by reporting entities, as required by c.29.2 (see relevant details in the analysis of R.29 in the TCA). This approach also ensures that CAMLMAC has access to all relevant details of key STRs to complement its own analysis of LVTRs and STRs. CAMLMAC reports the results of its analysis to the MPS or other competent authorities at central level, or passes the information on to the AMLB or a PBC provincial branch for an administrative investigation. The Head of the CAMLMAC takes the final decision in terms of dissemination to central LEAs or passing a case on for an administrative investigation. CAMLMAC also conducts jointly with the AMLB analysis of complex cases identified and transferred to them by the PBC provincial branches. As of 30 June 2017, CAMLMAC had 103 employees.

129. While the AMLB is primarily a policy driven unit, it also has the power to conduct administrative investigations of STRs identified by CAMLMAC. In addition, the AMLB coordinates and steers administrative investigations with cross-regional aspects conducted by PBC provincial branches (AML Law, Arts. 8, 23 - 26). The AMLB has the independent power to disseminate the results of its administrative investigations to central or local LEAs and other competent authorities. As mentioned above, the AMLB and CAMLMAC conduct joint analysis of complex cases. As of June 30, 2017, the FIU division within the AMLB had seven employees.

130. [16] identified by local regulated institutions and whistle-blower reports. In addition to

16 Key STRs are defined as follows: (i) The transaction is evidently suspected of ML, TF, or any

the analysis/administrative investigation of these types of reports, the provincial branches are also responsible for conducting administrative investigations based on suspicious activit

on to the provincial branches (AML Law, Arts. 8, 23 26). During this process, the 36 branches have limited access to information collected, analysed and disseminated by the other FIU components at the central or local levels nor systematic coordination with any of these FIU components. Subsequently, the 36 provincial branches take independent decisions as to whether or not to disseminate the results of their analysis/investigation to local competent authorities. Each of the 36 provincial branches shares information on its disseminations with CAMLMAC to ensure that information on key STRs and related dissemination data are centralised. However, the branches keep process information and information collected during the analytical/investigative process, including the information of cases not disseminated, in a stand-alone database, which is not accessible outside the individual PBC branch itself (i.e., not to CAMLMAC, AMLB and other branches). In addition, and equally important, local LEAs work closely together with each of the 36 provincial branches and frequently send requests for information directly to the relevant branch. Upon receipt of such requests, the receiving branch enters them in its stand-alone database. CAMLMAC or any of the other branches have no access to information requests directly sent by LEAs to an individual branch and are thus completely unaware of the process and the information itself. CAMLMAC receives relevant information at the

its database. As of the end 2017, all 36 provincial branches together employed 90 specialized AML investigators.

131. The dissemination of all cases to LEAs and other competent authorities, both spontaneously and upon request, by each of the 36 PBC provincial branches requires the signature of the president of the branch. While the assessment team has no indication nor evidence that this requirement has led to any undue interference in the dissemination process, these requirements could however limit the independence of the FIU and delay the timely dissemination of analysis results. Moreover, this additional step in the dissemination process could delay disseminations to LEAs and

other criminal activity. (ii) The transaction seriously compromises national security or affects social stability. (iii) Any other serious circumstance or emergency.

other competent authorities, which is of concern taking into account that key STRs by their nature are often urgent and highly suspicious.

Use of Financial Intelligence and Other Information

Use of Financial Intelligence and Other Information by the FIU

132. CAMLMAC receives STRs and LVTRs from all categories of FIs as its main type of financial intelligence, while the PBC branches are the primary recipient of key STRs from FIs. Reporting institutions also simultaneously send the information contained in use of the information to support its analysis of STRs and LVTRs. However, the lack of reporting by the majority of FIs and the absence of reporting by DNFBPs limits analyse and share accurate and timely financial intelligence. For more information and details on STR reporting and on coverage of DNFBPs, see Chapter 1 and IO.4.

133. CAMLMAC, the AMLB, and the PBC provincial branches have access to a wide range of financial, administrative, and law enforcement information, either directly or upon request. The AMLB and PBC provincial branches also have the power to obtain any relevant documents and materials from any reporting entity when conducting an administrative investigation. This broader power (which happens to correspond to technical requirements in R.29 (c.29.3)), does not extend to CAMLMAC. CAMLMAC only has the power to request a supplement and/or a correction from any reporting institution when an STR or LVTR is incomplete or erroneous. If CAMLMAC considers that a case file would benefit from additional information from reporting entities, then it has no other option than to transfer the case for an administrative investigation to the AMLB or one of the provincial branches. This approach limits is relevant for LEAs. This is a concern because CAMLMAC is the only component of ement and the only entity in the country with access to all STRs, information, see analysis on R.29 (c.29.3(a) and (b)) in the TCA.

134. CAMLMAC, the AMLB, and the PBC provincial branches have direct access to police databases for passport and other identification details. Each of the FIU components can obtain other police information beyond passport and identification

through liaison officers at relevant competent authorities; (iii) information from administrative sources such as, property ownership and social security information; (iv) whistle-blower reports; and (v) information from public databases. LEAs can obtain FIU data upon request. They do not have liaison officers at CAMLMAC, the AMLB, or any of the 36 provincial branches to facilitate this indirect access.

140. While LEAs have the power to request information from Customs on incoming and outgoing cross-border transportation of both national and foreign currency, the fact that collection and storage of relevant information by Customs is mainly paper based means that this type of financial intelligence is not readily available for use in

141. LEAs, both at central and local level, have the power to obtain financial intelligence from reporting institutions, either directly or via CAMLMAC and the 36 PBC provincial branches. To facilitate the receipt of financial intelligence from reporting institutions, LEAs at the central level, make extensive use of express inquiry and feedback channels directly with FIs, such as the dedicated Electronic Inquiry Platform with more than 60% of the commercial banks connected. Similar arrangements have recently been set up at the local level.

142. As set out in R.31 of the TCA, LEAs have the power to use special investigative techniques when conducting a financial investigation and the authorities presented relevant cases to the assessment team.

STRs Received and Requested by Competent Authorities

143. Since 2012, CAMLMAC, CAMLB and the PBC provincial branches have worked with FIs to reduce the volume of defensive reporting and improve the quality of STRs and key STRs. These efforts have resulted in a significant decrease in STRs reported to CAMLMAC (from 29.6 million in 2012 to 5.44 million in 2016) and an increase in key STRs directly and simultaneously reported to both the relevant provincial branch and CAMLMAC (from 4800 in 2012 to 8504 in 2016).

144. The large majority of (key) STR reporting (95%) takes place in electronic format and all relevant data a

the assessment team has no indication that CAMLMAC or the PBC provincial branches face challenges when entering the relevant data in their databases.

145. The fact that CAMLMAC directly receives the information contained in a key STRs simultaneously reported to the PBC provincial branches allows CAMLMAC to centralise the receipt of all types of reports (STR, key STR, and LVTR) by Chi arrangement. This is important because each of the 36 PBC provincial branches operate stand-alone databases, which are not accessible by CAMLMAC, the AMLB or any other branch.

146. FIs face challenges in determining whether they should report suspicions in the form of an STR or key STR. Representatives of FIs informed the assessment team that they would only report a key STR to a PBC provincial branch and CAMLMAC when they are able to identify an underlying predicate offence through the results of their detailed and substantiated analysis, which they also referred to as an investigation. Representatives of some institutions explained that in the absence of a predicate offence

They clarified that, in such cases, they would file a report in the form of a whistle-blower report directly with central or local LEAs but would not simultaneously file an STR or key STR with CAMLMAC and/or a PBC provincial branch. This is a concern because

proceeds of crime (POC) (see write-up of IO.4 for more details). Moreover, reporting entities are often not in a position to confirm that a suspicion is indeed associated with an underlying predicate offence because they have no access to law enforcement information. This means that some reporting entities provide possibly relevant

While this approach ensures that LEAs have access to suspicious activity identified by

to establish linkages with other data in its possession and to produce complete and meaningful financial intelligence that could otherwise assist LEAs in identifying new leads for investigation or support them in their ongoing investigations.

147. In addition to STRs and key STRs, CAMLMAC receives a high number of other reports because of the requirement for FIs to report LVTRs, including large-value cash transactions, large-value transfer transactions, and large-value cross-border transactions, based on a low threshold. For details regarding the threshold for LVTRs, see R.29 in the TCA. The number of LVTRs has been steadily increasing since 2012, reaching 4.94 billion in 2016.

Operational Needs Supported by FIU Analysis and Dissemination

148. All LEAs the assessment team met with during the onsite visit, both at the central level and in Shanghai and Shenzhen, informed the team that disseminations by CAMLMAC and the PBC branches are very helpful and often assist them in successfully completing predicate offence investigations. They also mentioned that financial intelligence from the FIU arrangement allowed them to initiate new predicate offence investigations. However, the statistics presented by the authorities do not fully support these oral statements. While these statistics show a 100% success rate of disseminations upon request (because CAMLMAC or the provincial branches is respond to each request received), the number of spontaneous disseminations, especially by CAMLMAC do not result in or contribute to a comparative large number of criminal investigations by LEAs. The following table gives an overview of the number of both spontaneous disseminations and disseminations upon request by CAMLMAC and the 36 PBC provincial branches, and an indication of how many of these disseminations resulted in or contributed to criminal investigations by LEAs.

149. In 2016, CAMLMAC disseminated a total number of 4121 cases: 720 spontaneous disseminations and 2701 disseminations in response to a request from LEAs. These 3421 cases contributed to/resulted in 2786 criminal investigations by LEAs: 85 because of spontaneous disseminations and 2701 in response to all of the

spontaneous disseminations only represent 3% of the total number of these criminal

s by

LEAs. The authorities did not provide any statistics to show how many of these 2786 criminal investigations with financial intelligence from CAMLMAC resulted in prosecutions and convictions because the focus of the statistics is on criminal investigations only. The authorities explained that the investigative process following FIU disseminations is long and feedback up on subsequent prosecutions and convictions is often not available.

150.

disseminations compared to its disseminations upon request is the high threshold that CAMLMAC applies for most of its spontaneous disseminations to LEAs, namely when it has a clear indication of a specific predicate offence. This shows to be a challenging approach taken by CAMLMAC, as one of the essential components of

to

disseminate meaningful financial intelligence to LEAs spontaneously. On the other hand, PBC provincial branches spontaneously disseminate relative higher numbers of files to LEAs compared to CAMLMAC, and this appears to be the direct result of the nature of key STRs, namely that this type of STRs received by the provincial branches often already include an indication of the predicate offence. It does therefore not establish that provincial branches undertake more extensive analysis, or analysis of a higher quality than CAMLMAC

151. In 2016, the 36 PBC provincial branches disseminated together a total number of 3599 to local LEAs: 1980 spontaneous disseminations and 1619 disseminations upon request. These 3599 disseminations contributed to 1905 criminal investigations by LEAs: 286 because of spontaneous disseminations (being on average eight cases per PBC provincial branch) and 1619 in response to the same number of requests from LEAs (being 45 cases per PBC provincial branch). This means that in 15% of the 1905 criminal investigations LEAs used financial intelligence from spontaneous disseminations while the other 85% were a direct

result of requests for information from LEAs. The authorities did not provide any statistics to show how many of these criminal investigations resulted in subsequent prosecutions and convictions as the focus of the statistics is on criminal investigations only. As mentioned above, the authorities explained that the investigative process following FIU disseminations is long and feedback up on subsequent prosecutions and convictions is therefore often not available.

152. The authorities presented the team with successful cases, including the following example, which demonstrates a successful dissemination upon request by one of the provincial branches.

> This case is an example of the successful conclusion of both a predicate offence and an ML offence investigation with the active involvement of a PBC local branch. In 2012, the Fuzhou Public Security Agency investigated
>
> During the lifetime of the investigation, the Public Security Agency
>
> branch. The provincial branch identified the involvement of 8 banking institutions and 18 of their customers, each with dozens of accounts. The stance clarified the source and destination of the proceeds from the predicate offence and provided important evidence for solving the case. The Public Security Agency also identified that another person W and other individuals were involved in laundering
>
> X for defrauding public deposits and W for ML but the authorities did not provide the assessment team with details on the sentences

153. When the PBC provincial branches are not in a position to confirm a predicate offence purely based on a key STR, they have the option to open an administrative investigation. During this process, they have access to additional information from reporting entities as well as administrative and law enforcement information (see core issue 6.1 for more details). However, the PBC provincial branches have only

data from CAMLMAC. Authorities explained that they take this approach to ensure that dissemination of information, if any, takes place as quickly as possible after the receipt of the key STR, and requesting information from CAMLMAC would delay the dissemination of financial intelligence. Direct access to the entire CAMLMAC database, including all LVTRs, would therefore address part of the concerns set out above (stand-alone databases at the other provincial branches remain inaccessible) and add value to the financial intelligence package.

154. PBC provincial branches would request CAMLMAC for assistance in more complicated cases, as illustrated by the following case example. This case example also illustrates that LEAs use disseminations by CAMLMAC and the PBC branches for successfully investigating and prosecuting predicate offences, as opposed to ML offences, as set out above.

This example points to the use of financial intelligence for the conclusion of a predicate offence investigation/prosecution with the active involvement of both CAMLMAC and a PBC local branch. In 2013, a bank in Tianjin filed

administrative investigation and concluded that the suspicious transactions were likely to involve illegal business activities, such as underground banks. Given the importance and complexity of the case, the provincial branch transferred the initial results of its administrative investigation to CAMLMAC for further analysis and input. CAMLMAC conducted data mining and transaction analysis and subsequently disseminated a number of cases to the MPS (number unknown). The public security agencies at the local level investigated the case based on suspicions of illegal business operations. Through the investigation, the public security agencies identified a large underground banking case, wound up 10 underground banks, and froze 264 bank accounts for a total amount of nearly RMB140 billion. The local People's Court sentenced a number of individuals (number unknown) for crimes of evading foreign exchange monitoring and foreign currency purchase defrauding under Criminal Law Art. 190..

opportunities to identify ML operations through targeted operations against underground bankers. See IO.7 write-up for more details.

156. Unless a PBC provincial branch explicitly requests CAMLMAC for assistance, as illustrated by the example above, there is no systematic interaction between CAMLMAC and the 36 PBC provincial branches upon the receipt of a key STR. CAMLMAC is therefore unaware of the action, if any, the branch takes in response to a key STR, unless the branch spontaneously disseminates the key STR and its associated analysis to the local LEAs, and subsequently makes relevant information

branches operates a stand-alone database, which CAMLMAC or any of the other 35 provincial branches cannot access, as set out in detail in core issue 6.1 above. Authorities do however not see this fragmented approach as an impediment for effectiveness because CAMLMAC also receives the information contained in each key STR to the provincial branch, and receives information on a subsequent dissemination, if any, by the provincial branches. However, CAMLMAC does not have access to information collected at a specific PBC provincial branch unless the branch makes these details available to CAMLMAC following its dissemination. Nor would CAMLMAC be aware that a branch is working on a key STR or responding to a request from LEAs, and what other information the branch has to its disposal. Similarly, the branch would not know if any of the other 35 branches or CAMLMAC would be working on cases related to the same subject, nor if CAMLMAC would have any relevant LVTRs in its database.

157. The simultaneous reporting of STRs to CAMLMAC and the information on a subsequent dissemination by the provincial branches indeed present concrete opportunities for CAMLMAC to add value to the financial intelligence chain. In practice, this does not seem to happen systematically for the following reasons. While CAMLMAC receives all information contained in a key STR and includes it in its database for use in future analysis, it does not proactively check its database for linkages with STRs, key STRs or LVTRs. Nor does CAMLMAC give any specific follow-up to a dissemination report it receives when a local branch disseminates a case based on key STRs. While one would expect that a dissemination of key STRs by a local branch would trigger the subsequent dissemination by CAMLMAC of any associated STRs, key STRs and LVTRs in its database, this is not the case.

158. Similar impediments arise when LEAs send requests for assistance to the PBC provincial branches. While the receiving PBC branch introduces the details of such requests in its own database, this information is not available to CAMLMAC or any other branch for use in their own analyses because they are simply unaware of the relevant law enforcement information. CAMLMAC receives a copy of all the disseminations upon request for inclusion in its own database but, as with spontaneous disseminations, CAMLMAC does not give any specific follow-up to these disseminations. This approach severely limits the analytical processes in place, prevents the development of a holistic view, and ultimately limits the relevance of the mpetent authorities.

159. When the provincial branches suspect or identify linkages with other provinces they can refer a case for joint analysis by CAMLMAC and AMLB or request the AMLB to initiate an administrative cross-provincial investigation. From 2014 to 2017, the AMLB initiated 1193 such inter-provincial administrative investigations involving various branches, or nearly 300 administrative investigations per year. However, it is not clear what disseminations, subsequent investigations, and prosecutions and convictions, if any, followed from this, making it impossible to assess the effectiveness. Moreover, in 2017, the AMLB and CAMLMAC performed joint analysis in complicated cases that led to 63 spontaneous disseminations. These 63 disseminations all resulted in subsequent investigations by LEAs and other competent authorities; however, it is unclear how many of these investigations resulted in prosecutions and convictions, which equally prevents the assessment of effectiveness.

160. As mentioned above, CAMLMAC receives a high number of other reports because of the requirement for FIs to report LVTRs based on a low threshold. The large volume and filing of LVTRs has a high potential to become useful for intelligence operations through operational and strategic analysis, following larger money trails and identifying wider networks. The authorities provided the assessment team with 13 cases in which the LVTRs reported to and analysed by CAMLMAC resulted in/contributed to successful criminal investigations by LEAs and subsequent prosecutions and convictions. Eleven of these cases clearly show that CAMLMAC successfully uses LVTR data to support its analysis of STRs and subsequent disseminations, and to respond to requests from LEAs. One case also showed how CAMLMAC initiated and successfully completed in-depth analysis of LVTRs based on information received from foreign counterparts. The two other cases provided

evidence that CAMLMAC conducted datamining of LVTRs and identified involvement in predicate offences and this led to the dissemination of these cases to LEAs and supervisors respectively.

161. Both CAMLMAC and the PBC provincial branches produce strategic analysis. They primarily issue these products to guide FIs in their identification of ML/TF risks and facilitate the (key) STR reporting regime. For example, they published documents to guide FIs in their monitoring and analysis of illegal fundraising and TF activities. They also issued various ML risk reminders on the latest trends in and characteristics of ML/TF activities. These risk reminders thus also assist FIs to increase the quality of STRs and this would ultimately result in higher quality financial intelligence. In addition to the documents produced for reporting entities, both CAMLMAC and the provincial branches issue so-called national and regional ML analysis and research reports to raise awareness of and provide policy guidance to LEAs and other competent authorities on new trends and typologies. C.29.4(b) requires strategic analysis to use available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns. The limitations presented by the stand-alone databases at the level of the 36 PBC provincial branches and the limited access by

effectiveness of strategic analysis processes. As pointed out in IO.1, the strategic analysis products did, so far, not result in any significant changes in terms of ML and TF investigations but provided useful contributions in terms of predicate offence investigations.

162. The statistics provided to the assessment team show that in 2016, CAMLMAC and the PBC provincial branches identified and spontaneously disseminated 412 instances of TF (176 by CAMLMAC and 236 by provincial branches). During the same year, LEAs initiated 147 TF investigations. The authorities were unable to provide a concrete indication of how many of these 147 investigations resulted from the 412 FIU disseminations but clarified that they believe that 20-30% (or 29 to 44 cases) were initiated based on FIU information. The origin of the other 70% is unknown.

163. The authorities provided several examples of TF investigations and subsequent prosecutions and convictions following spontaneous disseminations and disseminations upon request by both CAMLMAC and the provincial branches. The example below involving CAMLMAC shows that financial intelligence produced by

gement clearly has the potential to offer added value for use in TF investigations.

In 2014, a financial institution reported to CAMLMAC that account presented suspicious transactions. The credit transactions consisted of numerous cash deposits at ATMs in those regions of China where the Eastern Turkestan Islamic Movement (ETIM) operates. Despite the very high fees charged for cash withdrawals abroad, the debit transactions mainly consisted of cash withdrawals at ATMs in Malaysia and Turkey, but also in other regions of China. In mid-July 2014, the account became dormant. Intelligence from the police showed that Mr. A had left China for Turkey.

the financing methods of the ETIM and CAMLMAC therefore included an indicator in its database that would trigger an alert upon receipt of additional (key) STRs or LVTRs. In June 2016, after two years of inactivity,

bank again reported these to CAMLMAC. The STRs immediately triggered

also consisted of international transfers via an underground bank, also under monitoring by CAMLMAC. In addition, CAMLMAC had the beneficiaries of the various transfers on record for suspicion of terrorism financing. On that basis, CAMLMAC disseminated the case to the competent LEA. In the course of the subsequent investigation, the police identified another individual Mr. M. who confessed to act on behalf of Mr. A. Mr. M was subsequently charged with the TF offence and sentenced to more than one decade in prison.

Cooperation and Exchange of Information/Financial Intelligence

164.

arrangement and LEAs have mechanisms in place to allow for the sharing of financial intelligence and other information, as described in previous paragraphs.

165.

Electronic Exchange Platforms to facilitate online requests, assistance and feedback on use of financial intelligence. CAMLMAC, the MPS, the Ministry of Industry and Information Technology, and others also jointly established a platform for the

3

the authorities provided the assessment team with a case example showing how CAMLMAC initiated in-depth analysis of LVTRs based on an information request received from one of its foreign counterparts, and subsequently completed with information from a third FIU. Despite this positive outcome, which is very welcomed by assessors, feedback from the global network pointed to weaknesses in the scope of assistance that CAMLMAC is able to provide. As mentioned above with regard to core issue 6.1, CAMLMAC does not have the power to request information from any reporting institution. In addition, fundamental deficiencies in availability of BO information in China also have an impact on the exchange of financial intelligence with foreign counterparts, and the effectiveness of such exchanges and the production of financial intelligence more broadly.

169. In November 2016, CAMLMAC set up a special cooperation mechanism with the Australian FIU AUSTRAC. CAMLMAC and AUSTRAC share financial data on a monthly basis. CAMLMAC screens all key STRs for links with Australia and makes these data available to AUSTRAC. On the other hand, CAMLMAC conducts analysis of STRs it receives from Australia in view of dissemination to LEAs.

Overall Conclusions on Immediate Outcome 6

170.

ML Identification and Investigation

171. The MPS is the government ministry with responsibility for law enforcement. The MPS has subordinate Public Security Bureaus (PSB) at provincial and municipal levels with sub municirosecuitcome 7 (ML

172. The General Administration of Customs (GAC) is the border agency which supervises inbound and outbound activities. Within the GAC is the Anti-Smuggling Department, which can investigate ML associated with customs-related crimes. Generally, upon detection of ML activities, matters are referred to ECID.

173. Investigators within the newly formed National Supervisory Commission (NSC) (formally the Central Commission for Disciplinary Inspections (CCDI) and the Bureau of Anti-Corruption and Bribery of the SPP) have the mandate to undertake specialized investigation of suspected misconduct by public officials. Suspected ML identified by CCDI is referred to public security bureaus for investigation.

174. The SPP has a national responsibility for prosecution of ML and predicate crimes. The SPP exercises authority over prosecutions, reviews investigations, determines evidential sufficiency for prosecution, and oversees the activities of the public security agencies, as required. The SPP is an agency that comprises trained legal practitioners, who present prosecutions to the SPC and the subordinate courts. The SPP have an important role in that prosecutions only advance to the courts upon

to the PSBs. Such administrative agencies routinely refer matters to PSBs.[20] In 2017, the Central Committee of CPC and State Council reaffirmed a commitment to fight ML and tax evasion[21] and mandated that agencies should work in close collaboration.

176. The crime of ML is criminalized under three discrete articles of the Criminal Law Arts. 191, 312, and 349, each having a distinct application. Art. 191 addresses the behaviour of laundering the proceeds of a specified range of offences. Art. 312 covers the laundering of proceeds generated from any crime subject to a minimum threshold or particular conditions. Thresholds are established at the discretion of each province within a range of not less than RMB 3 000 (USD 440) and not exceeding RMB 10 000 (approx. USD 1 467). Current thresholds implemented in each province of China range between RMB 3 000 (approx. USD 440) and RMB 7 000 (approx. USD 1 027).[22] Art. 312 also criminalises the offence of the receipt or receiving of property derived from crime. Art. 349 relates exclusively to the harbouring or disguising of pecuniary benefit derived from narcotic crime (which could also be captured under Arts. 191 or 312), but this offence also criminalises the behaviour involved in drug trafficking which extends to the harbouring, transfer, or concealment of narcotics (refer to R.3 of the TCA).

177. money; offence, whereas ML prosecutions occur with modest frequency. Authorities explained that it is a principle of Chinese law that where the offender (launderer) knew of their intended role to deal with proceeds, (a behaviour that would ordinarily be a contravention of an ML offence) prior to the completion of the predicate criminal behaviour, their ; they would therefore be prosecuted for the predicate crime. Authorities identified that this

20 Art. 3 of Provisions on Transferring Suspected Criminal Cases by Administrative Authorities obligates administrative authorities to transfer detected crimes to public securities agencies.

21 Opinion on Strengthening the Supervisory Framework and mechanism for Anti-Money Laundering, Combating the Financing of Terrorism and Anti-Tax Evasion (State Council GAD letter [2017] 84).

22 in the trial of criminal cases on cover-up or concealment of crime related income and proceeds 1) places values thresholds and other conditions on when this offence can be prosecuted.

strategy also ensured a harsher penalty as the courts impose sentence in accordance with the most serious offence, which is generally the predicate. China confirmed that it would only be appropriate to charge an individual or a legal person with ML if it was proven that their knowledge as to the origins of property they dealt with, was acquired after the predicate criminal act was completed. Public security agencies, and representatives from SPP and the SPC confirmed this approach. This concept is understood, and it confirms that the limited prosecution of ML is due to China having a narrow focus on third-party launderers, who were not actively engaged prior to the

engaged to provide ML services after the occurrence of the predicate criminal behavior.

Consistency of ML Investigations and Prosecutions with Threats, Risk Profile and National AML Policies

178. Authorities have identified that significant proceeds are generated from high-risk predicate crime types and increasing numbers of predicate convictions for crime types such as illegal fundraising, tax crime, participation in pyramid selling schemes,

creasing focus on income generating crime. During 2013-2016, China identifies that 2.6 million persons were convicted of predicate income generating crime.

179. Given the number of predicate convictions and the geographical size of China, it is difficult for a

who provided ML services, but who were convicted for the predicate crimes. For this reason, statistical data that confirmed the existence of parallel investigations to identify and prosecute third-party launderers is limited to those persons convicted under the three ML articles being Arts. 191, 312, and 349.

23

predicate activities in China. Analysis of the Art.191 convictions (which targets the most serious ML offending) during the period 2013 2017, identifies that convictions against this article are increasing, but a comparison with the volumes of predicate crime highlights ML response using this specific article remains low. China acknowledges that the gradual increase in application of Art. judicial system being relatively conservative and therefore accepts the need to increase the awareness of the application of Art.191.

182. Illegal fundraising is the single highest income generating crime, reportedly contributing to approximately 39% of all illicit income generated in China. However, corresponding Art. 312 convictions (Ch predicated by this crime type comprise less than 1% of all ML prosecutions. Similarly, national strategic documents such as the NRA identify a current China policy focus on tax crime. During 2013 2017, there were 19 850 convictions for this crime type with comparative ML prosecutions predicated from tax crime being a relatively low 30 Art. 312 convictions.

183. Although it is accepted that additional ML behaviors will have been countries), the high incidence of predicate criminal behaviors all of which generate tens of billions of RMB, confirm considerable ML activity is not being investigated and appropriately prosecuted.

184. Autho an ML offence remains challenging. SPC issued an interpretation in 2009 to assist Investigators, the Procuratorates, and the Courts inferred from objective, factual circumstances. However, as a result of discussions on site and from a review of statistics, it is clear that this interpretation has had limited impact on the use of the ML Articles.

185. The prevalence of underground banking is a concern to Chinese authorities. The NRA identifies that underground banks (together with cross-border cash smuggling) is a preferred channel to remit illicit proceeds offshore. In 2016, public security agencies investigated 380 underground banking networks, arresting over 800 persons involving transactions exceeding RMB 900 billion (approx. USD132 billion). Throughout the onsite visit, authorities made numerous reference to the use of underground banking networks to launder criminal proceeds (and assist in the movement to TF funds). However, with limited exception, it was expressed that

investigation and prosecution of various types of ML activities, including three cases of ML with a foreign predicate offence, third-party ML, and stand-alone ML have occurred, but in context of risk and predicate crime, convictions occur with insufficient frequency.

188. Regarding the prosecution of ML associated with foreign predicate offences, in 2005, a Chinese citizen was convicted for the laundering of funds that were derived from predicate activities that occurred in Malaysia. This individual was sentenced to imprisonment and fined RMB 330 000 (approx. USD 48 430). More recently, two additional examples of prosecution associated with a foreign predicate crime have occurred both resulting in successful convicted pursuant to Art. 312. Most of the limited Art. 191 prosecutions emerging out of domestic drug, corruption, and fraud-related crime. The subjects of these prosecutions are often a family members or close associates of the predicate offender.

189. The following are examples of ML cases, linked to narcotics, corruption and illegal fundraising.

: J assisted his cousin with laundering the proceeds of ephedrine sales. J established companies in false names, he also established two liquor companies and a second-hand car dealership through which the illicit proceeds were laundered to the value of RMB 11.2 million (approx USD 1.64 million). On September 16, 2015, J was convicted of ML, sentenced to 600 000 (approx. USD 88 056).

: B engaged the services of his sister, Y, and his brother-in-law, H, to receipt his drug-dealing income through their banking facilities. Y received RMB 10 950 (approx. USD 1 607), and H received RMB 8 000 (approx. USD 1 174) with the knowledge that their bank facilities were being used to disguise the illicit source of B
convicted of ML and sentenced to one-and-a-
fined RMB 2 000 (approx. USD 293), H was sentenced to one-year

(approx.. USD 146).

190. A number of other drug-related case reviews identify the use of Art. 312 to prosecute the concealed possession of criminal proceeds, such as possessing proceeds of crime on behalf of, and for the benefit of, a person involved in predicate criminal activity. In relation to Art. 349, case reviews identified that this article was

used to prosecute persons who held narcotics for safekeeping on behalf of another, a behaviour discrete from ML.

191. Corruption is a recognised predicate crime in China, and authorities have made commendable efforts in combating this problem. ML prosecutions identified in relation to this crime type largely involved family members and close associates of the predicate offenders. No cases were reviewed that involved corruption and bribery activities that were occurring in foreign jurisdictions.

: Z received funds from his Uncle L, who was a mayor and Municipal Party Secretary, with the knowledge that the funds were the proceeds of corruption. Upon receipt of the funds he invested them in a property development on behalf of his uncle. On August 18, 2016, Z was convicted in

fined RMB 1.1 million (approx. USD 161 437). Z appealed the conviction

: L received bribery proceeds to the value of RMB 200 800 (approx. USD 29 469) from his brother-in-law who was a senior official in the Agricultural Mac
bank accounts, and he undertook various financial transactions and acquired vehicles on instruction of his brother-in-law. On December 18, 2014, L was convicted for corruption and ML and sentenced to six months imprisonment and fined RMB 20 000 (approx. USD 2 935).

192. Illegal fundraising is identified by China as a high-risk income-generating predicate crime and considerable enforcement activities had occurred to combat this crime type.

: L was the cousin of a subject who without the approval of the National Financial Regulatory Authority raised funds from the general public amounting to RMB 175 million (approx. USD 25.7 million). With knowledge that funds were illegally raised, L permitted the use of personal bank accounts for the purpose of managing the funds. On July 21, 2016, L was convicted of ML and sentenced to two years and three months and fined RMB150 000 (approx. USD 21 936).

: Between 2008 2001, funds were illegally raised from the public promising a high yield of return. The principle offender transferred RMB 100 million (approx. USD 146 million) to Z, his ex-wife. On August 10, 2017,

Z was sentenced to seven years imprisonment and fined RMB 40 million (approx. USD 5.9 million) for ML

193. A review of 93 ML case examples provided by China demonstrated that there is the capacity to effectively investigate these predicate offences; however, statistics confirm that investigation efforts are not consistently aligned to risk.

Effectiveness, Proportionality and Dissuasiveness of Sanctions

194. In addition to the previously referenced legal issues, authorities identified that the modest number of ML prosecutions reflected their desire to pursue the

investigators and prosecutors identified that stand-alone ML prosecutions resulted in lower punishments when contrasted with the punishments for predicate offences. The team, however, considered that the sanctions available are effective, dissuasive, and proportionate, given that ML offences each have a maximum sentence of up to 10

-related measures.

195. An analysis of sentences from the case reviews evidenced that most

Confiscation of Proceeds, Instrumentalities and Property of Equivalent Value as a Policy Objective

197. China, through policy, law, and strategy, demonstrates a commitment to pursue and confiscate criminal proceeds through both criminal and administrative proceedings. The State Council recently issues an Opinion on Strengthening the Supervisory Framework and Mechanism for AML/CFT and Anti-Tax Evasion that reinforced the resolve of the country to pursue the recovery of criminal proceeds as a national policy objective.

198. The Criminal Law of China reflects this intent with Arts. 59 and 64 providing legal authority to confiscate criminal proceeds and any property used in the commission of criminal activities and

constituted a domestic ML offence. This was a significant undertaking for China demonstrating effective international cooperation. In 2016 final resolution resulted in the forfeiture of NZD 43 million (approx. USD 29 million), which was shared between New Zealand and China, pursuant to a sharing agreement

199. Operation Foxhunt has led to positive results that Chinese authorities are able to cooperate with foreign authorities to extradite criminals and recover illicit proceeds, which is relevant for this immediate outcome. That said, much of the property recovered as a result of Operation Foxhunt is as a result of persuasion (as it is referred to in Chinese media) and negotiations directly between the fugitive and Chinese authorities, which is outside the scope of the requirements of the standard.

200. The criminal procedure law implemented on January 1, 2013 established the special confiscation provisions of Art. 280, allowing confiscation of property without a criminal conviction where the criminal suspect or defendant escapes, hides or dies. In January 2017, China released a judicial interpretation on the special confiscation procedure to promote the applicatio

expressly described in law (according to the SPC during the on-site), this interpretation, together with the general sentencing guidelines, in practice provide for equivalent value confiscation.

202. Based on a SPC, SPP and MPS notice, during the course of a criminal investigation, public security agencies can seize or legally preserve property, including real estate, vehicles, and other property of value along with any legal documents and instruments that prove ownership or rights. This process occurs when a criminal investigation is registered as an investigation case or a prosecution has been initiated. Appropriate ministries are advised, such as the MOHURD, who provide support to administer the seizure or preservation authorisation. The authorisation remains in force until resolution of the criminal proceeding.

203. In addition to criminal forfeiture, administrative forfeiture is applied for behaviours that do not constitute criminal behaviour in Chinese law. This forfeiture is applied by various administrative authorities such as the SAT or routinely the GAC. Further, administrative agencies, when not permitted by a specific law, can (based on the Administrative Coercion Law) apply to the court for enforcement measures which can include freezing and seizure authorities, as sanction for administrate violations.

204. Property that is seized is retained by the Public Security Agency or under

circumstances, property can remain in the custody of the owner or close family, subject to certain conditions that protect the value of the property.

Confiscations of Proceeds from Foreign and Domestic Predicates, and Proceeds Located Abroad

205. The legal processes and the various interpretations evidence policy objectives and provide a sound legal framework for the confiscation of criminal proceeds. Emerging crime threats have resulted in the development of several electronic enquiry platforms to allow public security agencies and the courts to directly enquire with banks to freeze funds and suspend the operation of accounts in response to increased occurrence of some crime types such as telecommunications related frauds. Public security agencies are routinely using this platform upon receipt of complaints to recover victim funds and to assist with such investigations. As of March 2018, there were 39.1 million inquiries, resulting in RMB 202 billion (approx. USD29.7 billion) of deposits being frozen, pending investigation.

206. Police officers across the public security agencies can initiate seizure and freezing upon the approval of PSB leaders. Approximately 18 000 dedicated specialists in various LEAs are engaged in the function of asset tracking and confiscation; and authorities themselves are of the view that prosecution and judicial agencies are all adequately skilled and resourced to initiate and undertake confiscation functions.

207. Statistics provided by China confirm that confiscation is being applied routinely to crime types including those recognised as high risk. During 2013 2017, confiscations valued at RMB 123.2 billion (USD 18.1 billion) have been identified from publicly available judgements. There are additional judgements which are suppressed and therefore the likely confiscation value would exceed this value. These forfeitures are primarily achieved through three discreet forfeiture processes instruments of crime (property which facilitates offending); direct proceeds of crime; and forfeiture of property which is applied to satisfy fines imposed to reflect equivalent value confiscation.

208. Confiscated instruments of crime between 2013-2017 were valued at RMB 288 million (approx. USD 42.3 million) from 192 715 cases. It is noted that instrument confiscation associated with ML pursuant to Art. 312 averaged RMB 3 621 (approx. USD 531) per case, and corruption cases average RMB 190 (approx. USD 27.80), reflecting that instrument confiscation values on a per case basis, were negligible.

213. Art. 395 was introduced in response to risk and to complement policy objectives in China. Persons (both natural and legal) who are involved in ML and the high- subject to a similar response, despite risk and the probability that the persons who professionally operate and provide underground banking services in particular are likely to have derived considerable income through fees received in the provision of underground banking services. The investigative challenges presented by underground banking activities also extend to foreign law enforcement when attempting to reconstruct financial events and track illicit income back to predicate crime occurring in China. Assessors discussed with authorities strengthening efforts through expanding the application of Art. 395 to underground banking and to reduce its prevalence.

214. Requests from foreign jurisdictions are enforced at the discretion of the Chinese authorities. Prior to the on-site an agreement of reciprocity was mandatory for China to co-operate with foreign jurisdictions to recover proceeds of crime.[25]

> In March 2016, France sought the assistance of Chinese authorities to recover the proceeds of a series of frauds that were contained within a Chinese commercial bank. Chinese authorities immediately froze accounts to a value of EUR 5.8 million. China and France are in current negotiations as to how to return these funds to the victims

[25] On October 26, 2018, Š ‡ ƒ ™ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ‡ ’ — „ Ž ‹ … ‘ ˆ Š ‹ • ƒ ‘ • • – ‡ ” • ƒ – ‹ ‘ • ƒ Ž Assistance came into force which allowed China to conduct judicial assistance and confiscation with foreign jurisdictions without an agreement of reciprocity, and provided China with a more complete domestic legal framework for international cooperation in confiscation.

215. China has developed processes to manage and dispose of property confiscated. In accordance with the Law of Administrative Penalty (Order of the President No. 76). Property confiscated is sold by public auction with the funds obtained turned over to the central or local treasury in accordance to law. Currently, 3 290 courts in 32 provinces dispose of confiscated property via online auction. The total value of confiscated property sold via the Ali Judicial Auction Platform was RMB 580 billion (approx. USD 85 billion), and authorities report that this platform is proving to be a highly efficient disposal mechanism.

Confiscation of Falsely or Undeclared Cross-Border Transaction of Currency/Bearer Negotiated Instrument

216. The movement of cash out of China is considered a main risk by the Chinese authorities, and the flow of illicit proceeds from China has also been identified as a risk in third-party countries.[26] China has currency control measures which regulate the amount of funds an individual can remit from China, but these are currency control restrictions that were not set up for AML/CFT purposes. Authorities identify that bearer-negotiable instruments are not able to be transacted in China and are therefore not subject to any regulation. This is a gap, considering that bearer negotiable instruments (such as checks) exist in China. China Customs website l cheques or letters of ng China which allows China to be a transit country for the movement of such financial instruments.[27]

217. In response to the growing use of Chinese debit cards in Hong Kong, China (said to be caused by the introduction of ATMs with facial recognition in Macau, China), Chinese authorities further restricted the use of domestically issued debit cards abroad to RMB 100 000 (approx. USD 14 675) per individual per year (instead of per account per year), (Regulation Hui Fa 2017/29 of January 1, 2018). According to the authorities, AML concerns justified taking these restrictive measures. However, these new restrictions were not complemented by specific AML/CFT measures, such as alerting relevant customs units that there would be a higher AML/CFT risk of

26 See for example the FATF/APG MERs on Australia, Canada (undertaken by the IMF), and Singapore.

27 See english.customs.gov.cn Customs Clearance Guide for International Passengers August 2, 2018.

increased flows of cross-border movements of cash between Shenzhen and Hong Kong, China. This lack of a focused AML/CFT policy approach regarding cross-border flows of currency, negatively impacts the effectiveness of the system. That said, the authorities have shared a general notice issued around the same time that alerted customs staff of the risk of cash smuggling (but not specifically of the increased risk of ML/TF).

218. Hundreds of millions of persons enter and exit China annually, for example 43 million person movements occurred entering and exiting Shanghai in 2017. China has implemented controls such as the (x-ray) inspected of all luggage, which in Shanghai has resulted in the detection of 170 cases of persons failing to declare currency in contravention of the declaration regulations. This detection rate is modest given the NRA identifies the cross-border carriage of cash is a risk China-wide, during 2013 to 2016, China Customs detected 2887 cross-border currency cases resulting in the confiscation of RMB510 million (approx. USD74 million). Upon detection, most cases result in an administrative confiscation.

219. Customs has a range of resources and technologies available to detect cross-border movement of cash, precious metals, narcotics, and counterfeit products. Given that movements of persons and freight are however large and the borders lengthy, Customs face considerable and significant challenges. Detections and the receipt of declarations are not submitted to the CAMLMAC in a timely manner (currently it occurs six monthly) to enable inclusion of such financial information in the process of

Key Findings

TF investigation and prosecution (Immediate Outcome 9)

a) China has an institutional framework in place to investigate and prosecute

previous legal framework (which was absorbed by the CTL) had not been used since 2012.

d) FIs seem not fully aware of the risks that TF can pose, and that TF and terrorism risks are not identical, especially in relation to the need to identify assets of designated entities. This is somewhat worrisome with respect to the larger financial centres.

e) is significant with nearly 800 000 social organizations registered at various government levels under the MCA. With the passage of – Š ‡ Š ƒ ” ‹ – › ƒ ™ ‘ ˆ – Š ‡ ‡ ‘ Ž in 2016, China started the process of applying additional requirements on a subset of the sector that is involved with raising public funds to carry out charitable activity. None of the measures taken thus far however is based on an understanding of the risk of TF faced by such organizations and no aspect of the oversight mechanism relates to ensuring that such organisations are not abused for the purposes of TF.

Targeted Financial Sanctions Related to PF (Immediate Outcome 11)

a) Authorities are in the process of contemplating a law on PF but in the absence of a general legal framework that comprehensively covers all aspects of TFS requirements, the PBC has made a positive attempt to impose some measures to comply with some UNSC designations for the FIs.

b) The implementation of TFS is negatively affected by three fundamental deficiencies, related to (i) scope of coverage of the requirements and a lack of a prohibition covering all persons and entities, (ii) the types of assets and funds of designated entities that can in practice be frozen, and the type of transactions that can be prohibited, and (iii) a lack of implementation without delay.

c) There is a lack of awareness of Iran-related sanctions, with an almost exclusive focus by authorities and private sector on DPRK.

d) Despite the fact that authorities such as PBC are treating PF in relation to DPRK as an important issue, the AML/CFT shortcomings in CDD (IO.4) and supervision (IO.3) are nevertheless largely apply in relation to CDD and supervision in relation to PF shortcomings in this immediate outcome,

e) While not covered by the FATF standards, authorities have taken measures in relation to other aspects of UNSCRs related to DPRK that seem to be positive, and that may have a positive impact on the fight against PF in China.

Recommended Actions

TF Offence (Immediate Outcome 9)

a) China should enhance its mitigation of TF risk through a detailed analysis of the investigations and prosecutions of TF cases it has already conducted. Such analysis should include a breakdown the methods of TF, such as the collection, movement, and use of funds or assets. In addition, the analysis

should identify and categorize the various roles played by the individuals and legal entities involved in the financing of terrorism. Resources should focus on TF and terrorism cases, and on a more comprehensive focus on the seizure of criminal assets, including overseas.

b) In order to improve the detection, prevention, and prosecution of TF crimes, China should keep up-to-date and detailed statistics relating to TF offences and share this intelligence with LEAs and reporting entities through ongoing training.

c) To better mitigate the full range of system, China needs to broaden its TF focus and pursue cases of TF elsewhere in the country, particularly in its financial centres.

Targeted Financial Sanctions Related to TF and non-profit organizations (Immediate Outcome 10)

a) Authorities should create a comprehensive legal framework for the implementation of preventive TFS that covers all persons and entities, includes a general prohibition and can cover all assets and transactions. The existing CTL, if broadened in scope, could be a good basis for the implementation of both sets of UNSCRs.

b) In the interim, PBC should amend Notice 2017/187 and require FIs and DNFBPs to freeze the assets of UNSC designated entities as soon as designated by the UNSC. The MFA should continue to strive towards reducing the amount of time required to circulate UNSCRs (and amendments to lists) to relevant government bodies, such as PBC and CBIRC, to ensure that the entire process from designation by the UNSC would be without delay (i.e., ideally within hours).

c) Authorities should effectively use preventive TFS in line with the country's risk profile for TF, as foreseen by the existing provisions in the CTL.

d) Once a framework is in place, authorities should provide outreach to other (regional) competent authorities and the public to sanitize all relevant stakeholders about TFS.

e) China should determine the nature of threats posed by terrorist entities to NPOs, identify those organizations within the broader sector that, based on their activities and characteristics, are at risk of TF abuse and conduct outreach specific to the risk of TF abuse.

f) China should reconsider its position on placing AML/CFT obligations on all NPOs, identify the subset of NPOs within China that meet the FATF definition of an NPO and focus on raising the awareness of those organizations through outreach in order to protect NPOs from the threat of TF abuse.

Targeted Financial Sanctions Related to PF (Immediate Outcome 11)

a) Authorities should create a comprehensive legal framework for the implementation of preventive TFS that covers all persons and entities,

includes a general prohibition and can cover all assets and transactions. The contemplated law on PF could be instrumental in this regard.

b) In the interim, PBC should amend Notice 2017/187 and require FIs and DNFBPs to freeze the assets of UNSC designated entities as soon as designated by the UNSC. The MFA should continue to strive towards reducing the amount of time required to circulate UNSCRs (and amendments to lists) to relevant government bodies, such as PBC and CBIRC, to ensure that the entire process from designation by the UNSC would be without delay (i.e., ideally within hours).

c) Authorities should broaden their focus on TFS beyond the DPRK.

d) Once a comprehensive legal framework is in place, authorities should conduct outreach to other (regional) competent authorities and the public to sensitize all relevant stakeholders about TFS.

e) Authorities should monitor the FIs and DNFPBs compliance with these measures and continue to focus on the possible misuse of front companies that facilitate PF TFS breaches.

223. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9 11. The recommendations relevant for the assessment of effectiveness under this section are R.58.

[illegible]

224. In the NRA, China identifies the ETIM also known as the TIM, as its major terrorist threat. ETIM operate also(from) abroad and is believed to have carried out terrorist attacks in the Xinjiang province; recruited and trained Chinese citizens outside the country; and smuggled them back into China to perpetrate terrorist acts. In addition to ETIM, the NRA identifies a limited terrorist threat posed by local

extremism.

225.

border to the Middle East to join international terrorist organi s

Chinese authorities did provide TF cases relating to foreign terrorist fighters, the TF risk posed by foreign terrorist fighters is not elaborated on. Estimates of the number of Chinese foreign terrorist fighters in Syria differ, one estimate by officials in state media referred for example to 300 such fighters in 2014.[28] Irrespective of the exact

28 See for example Global Times, 15 December 2014, www.globaltimes.cn/content/896765.shtml

number, the issue is a concern for the authority. Moreover, this also suggests that attention to the TF risk resulting from foreign terrorist fighters in China is warranted (see also for IO.10).

226. The NRA indicates that the source of terrorist funds is derived from support by personal and corporate sponsors; the sale of personal assets; the receipt of gifts from relatives and friends; from funds generated through business income (such as A [29] from religious believers; and, illegal activity such as robbery. The main source of this information is strictly confidential and is only shared among authorities that belong to National Leading Group and AML/CFT MC; however, cases presented are in line with the mentioned sources of TF funds. The NRA states that it

disruption of TF and terrorist activity.

”‘•‡…—–‹‘• ‘•˜‹…–‹‘• ‘^ ›’‡• ‘^ …–˜‹–› ‘••Profile•–™‹–Š–Š

227. offences are not broken down by the type of TF activity investigated. Assessors were advised that authorities could not elaborate on their CT/TF approach for security reasons. At a macro-level, the case information provided by authorities suggest that these prosecutions and convictions are consistent with part of the risk profile. prosecution and convictions related to TF offences are generally consistent with the

228. At a local level, LEA activity focuses mostly on preventive investigations and other administrative violations of CFT measures [30] that authorities consider to be related to terrorism or necessary to fight terrorism (but some are outside the scope of the FATF standards). For example, of 15 terrorism cases taken up by local security authorities in Shenzhen, only one related to terrorism, the others to unrelated (lesser) offences under the Counter Terrorism Law. When a major TF offence is detected, the case is often transferred to the courts of Xinjiang province, where the detected facts related to TF activities were committed or originated. Authorities in Shanghai and

but also see paragraphs 3 and 46 of this report for other estimates (around 60 persons per year).

29 A form of alms-giving treated in Islam as a religious obligation or tax.

30 Such as the requirement to provide passports when checking-in at a hotel.

Shenzhen advised that this further lowered the low number of TF investigations and prosecutions in their regions. Cases transferred to Xinjiang became inaccessible for the authorities in other regions.

229. China identified the risk of transferring funds overseas for TF activities which includes overseas withdrawal of cash using ATM machines; cross-border cash transit; and underground banking activities. The following case summaries provided by authorities detail(wal)45.996 (of)43.007 mthoriti detail(wal)45.996 (of)43.007 T3.16 re f* 843.04 (i)-

ò t r s y u ó

In December 2014, the PSB in Xinjiang was notified by an office in another province that a known terrorist from outside of China had transferred RMB 14 000 to YA in December 2013.

The PSB in Xinjiang began financial analysis relating to the transfer to YA. They consulted local and national databases, accessed security intelligence and analysed disclosures from the FIU related to other national security and criminal investigations dating back to 2013, linking YA to 133 of them. multiple TF-related disclosures.

An investigative task force was established made up of the Counter-Terrorism Department, the Economic Crime Investigation Department, the Technical Investigation Department, and the Cyber Security Department. The task force organised the case investigation work across police types, regions, and levels. They used conventional police investigative methods to identify household registration, passport information, and past behaviours of YA and those associated to him both in and outside of China. YA was identified as a sophomore university student.

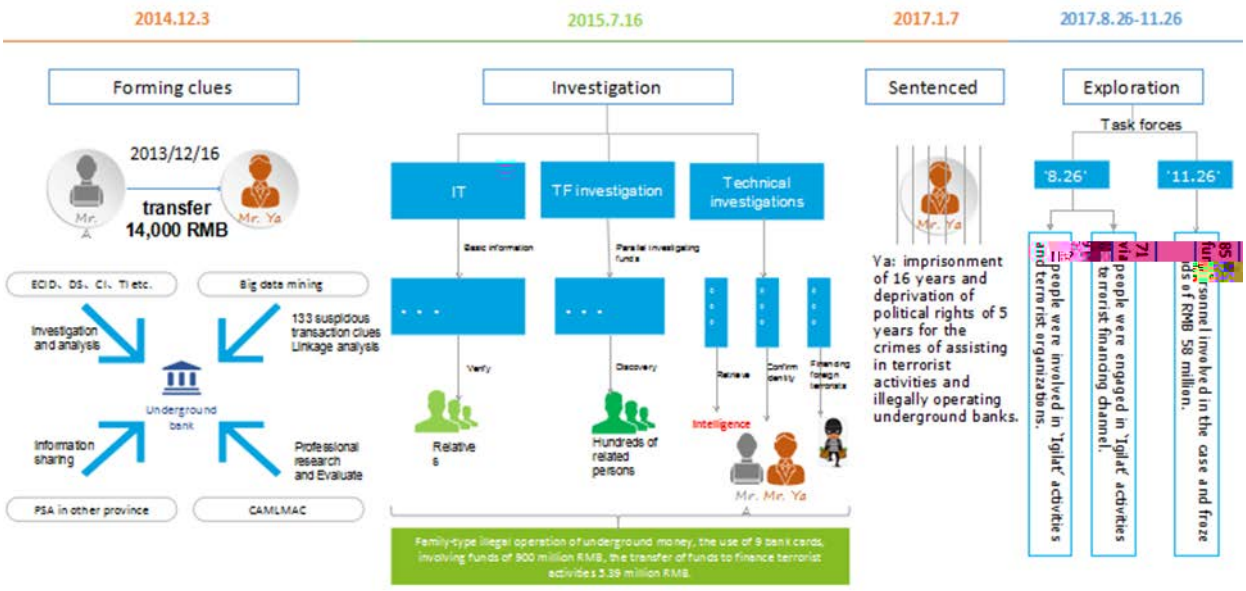
The local branch of the PBC was engaged to assist in the financial investigation expanding the analysis to over 100 accounts and 1 000 transactions. The analysis revealed a pattern of multiple large-value currency-
profile as a student. Funds tracking revealed hundreds of parties associated with YA, resulting in the belief that YA was involved in

transferring funds to terrorist organisations through underground banking channels.

The investigation involved monitoring of two mobile phones and six social media accounts belonging to YA revealing a network associated to ETIM and ISIL. Identities of the network were identified and confirmed through electronic surveillance. Transfers of funds, for the purpose of supporting ISIL, to AI, (identified to be an overseas member of a terrorist organisation) and SAI a key member of ETIM, were identified.

The investigation revealed that YA and his relatives operated companies and used them to cover the illegal operation of an underground bank. YA and his brother used nine bank cards to conduct transactions in excess of RMB 900 million, RMB 5.4 million of which was linked to TF activity related to travel for the purposes of fighting for a terrorist organisation.

The investigation into YA lead to the formation of other task forces to follow up on the TF transactions identified during the YA investigation. In January 2017, YA was sentenced to 14 years for TF and 3 years for operating an underground bank. In addition, RMB 20 million (the balance of the



TF Identification and Investigation

230. Identification and investigation of TF is a challenge for the authorities. China set up the National Leading Group for Combating Terrorism, which includes members from the SPC, the SPP, the MFA, the MPS, the MSS, the MOJ, GAC, and the PBC to mitigate terrorism and TF activities. The Economic Crime Investigation Department

(ECID) and Anti-Terrorism Department are the lead departments responsible for investigating TF in China.

231. MPS maintains a watch list of international and domestic persons and entities related to terrorism and TF. The full list is confidential (also the number of entities on the list) and only disseminated to LEAs and CAMLMAC. A shorter list is shared with FIs on a need-to-know basis to assist in STR generation. In 2014, PBC, with participation of CAMLMAC, PBC branches, the public security agency and the security department, developed a monitoring and analysis model and sub-models for TF transactions to assist AML/CFT reporting entities in detecting suspicious transactions related to TF.

232. Authorities indicated that, when necessary, investigations of complex terrorism and TF cases are carried out by forming special investigation task forces consisting of LEAs, State Security, the PBC and, in some cases, FIs. When dealing with international terrorism cases, China would co-operate and co-ordinate with international law enforcement and intelligence services. If required, TF investigations may include special investigative techniques such as wiretapping, internet surveillance, and undercover and special operations.

233. The following table provided by authorities represents the number of TF cases and the number of persons implicated in those cases. While the table represents a year-after-year increase in the number of TF cases, given the size of China and the identified risks of TF, the number of cases is relatively low. In addition, as mentioned earlier TF offences are not broken down by the type of TF activity investigated so it is not possible to determine the extent to which investigations identify the specific role played by the terrorist financier.

Source: AML/CFT Statistics China

234. The PBC advised that it provides guidance to entities with reporting obligations and promotes regular internal CFT training on TF. In addition, the PBC summarizes updates and gives indicators for monitoring funds

On this basis, FIs further study and develop monitoring models of STRs related to TF, mainly in electronic platforms for real-time scanning, that fit their own characteristics or needs. from submitted STRs and disseminate them to LEAs. The PBC routinely cooperate with investigations by participating in case discussions with LEAs and supporting ongoing investigations with analysis.

	±

TF Investigation Integrated with and Supportive of National Strategies

235. As mentioned, China has established a national coordination mechanism, The National Leading Group for Combating Terrorism, to coordinate overall planning of CTF strategies. The Office for the National Leading Group for Combating Terrorism was established by the MPS to enhance the coordination and promote effective operation of counter terrorism activity across China through supervision, guidance, monitoring and inspection. The members of the National Leading Group include the SPC, SPP, MFA, MPS, MSS, MOJ, SAC, and the PBC,

236. The National Leading Group for Countering Terrorism is responsible for

work plans for implicated departments. However, because operational plans are of a sensitive nature, involving classified national security issues, no information beyond high-level counter-terrorism strategic goals, and no information specific to CFT activities was shared with the assessment team.

Effectiveness, Proportionality, and Dissuasiveness of Sanctions

237. The following table, provided by the authorities, relates to sanctions imposed on natural persons convicted of providing assistance in terrorist activities. Given that such crimes may include administrative-type offences under the Counter Terrorism Law that are outside of the scope of the FATF Standard, and given that no specific

separate statistics can be provided (see above regarding the classification of TF related information for state-security reasons) it is not possible to determine that China has effectively imposed proportionate and dissuasive sanctions in TF cases. This negatively impacts the assessment. In addition to statistics, the authorities also provided case examples (which are partially consistent), with references to sanctions between three years and life, and a conviction of a legal entity. In addition, some cases presented indicate that in eight TF cases in 2017, assets were confiscated as an additional sanction (note that confiscation is generally assessed under IO.8).

Alternative Measures Used Where TF Conviction is Not Possible (e.g., Disruption)

238. If it is not practical to secure a TF conviction, authorities can carry out arrests, prosecutions, and trials in the name of other serious crimes such as accomplices of terrorist organizations, terrorist activities, terrorist training, harbouring criminals, assisting criminals, endangering national security, or other crimes such as the crime of disrupting order of the financial markets.

239. The following table, provided by the authorities, identifies the number of cases and implicated persons in crimes related to terrorist financing activities.

Source AML/CFT Statistics China.

prohibited. The authorities were unable to demonstrate that these other types of assets (e.g., real estate, land, cash), or other transactions, are effectively frozen or prohibited using other measures. This deficiency impacts the effective implementation of UNSCRs 1267 and 1373 as it allows designated entities to move their assets to safety.

- No implementation without delay (in relation to UNSCR 1267 and successor resolutions): Authorities were unable to demonstrate that the freezing actions that the PBC Notice provides for are implemented without delay (i.e., ideally within hours). The initial delays are caused by untimely circulation of new UNSCRs within the government, even before PBC and others could circulate the UNSCRs to supervised entities.

UNSCR 1267 and Relevant Successor Resolutions

243. Within the scope of PBC Notice 187/2017, the MFA is responsible for ensuring that UNSCRs are implemented in China. It is doing so by circulating relevant UNSCRs to relevant competent authorities, but consistent and timely circulation in all cases of UNSCR 1267 and successor resolutions and amendments to the lists of designated entities related to these UNSCRs, could not be demonstrated. Based on Notice 187/2017, the PBC is then responsible for following up on the MFA circulars by circulating the information on new UNSCRs to FIs (as a notices); but consistent and timely circulation in all cases could also not be demonstrated.

244. During the onsite period, the UNSC amended the list of 1267-related designations,[31] which provided an opportunity for competent authorities and FIs to establish, for the purposes of this assessment, that new designations and amendments to the lists are indeed circulated without delay. Assessors therefore checked with (regional) competent authorities and with FIs if they were aware of a

very recent change to the list of designations. This was not the case, interviewees were not aware of this recent change to the UN list, or of other recent changes to the UN lists. Assessors could therefore not confirm that UNSCRs (and amendments to designation lists) are indeed circulated and reach FIs without delay (i.e., ideally within hours).

245. FIs interviewed made references to commercial compliance software solutions as their main source of information. Indeed, PBC requires the use of commercial compliance software to mitigate the delays in circulation of the UNSCRs. This is a positive step, albeit not unique to China, and FATF has indicated that the use of commercial databases poses challenges.[32] The reliance on third-party software may also explain why FIs were not aware of recent amendments to the list by the UNSC. These commercial databases are said to be updated one day after the UN designation/amendment, but this was not verified. The compliance software solutions do not distinguish between UN, EU, US, or other sanction programs and some FIs suggested that they implemented all these lists in China, regardless of the issuing jurisdiction. Such a suggestion is problematic from a domestic legal point of view, although internationally operating FIs may have no choice but to try to comply with competing lists from different jurisdictions.

246.

There have been no other submissions to the UNSC since 2009. Possible other targets for preventive designation by the UN could have been Chinese foreign terrorist fighters fighting in Syria/Iraq or other ETIM members. That said, authorities also stressed that in case of the detection of any funds related to ETIM, authorities would likely prioritise criminal justice measures. While this does not assist in the implementation of this immediate outcome, it does positively impact IO.9 (see IO.9).

UNSCR 1373

249. Where applicable, issues that relate to UNSCR 1267 and successor resolutions as described above equally apply to the implementation of the TFS provisions of UNSCR 1373 and are not repeated in this subsection.

250. On the basis of a previous legal framework (that was absorbed by the CTL), China has domestically designated 4 organisations and 25 persons as terrorists, in 3 tranches in 2003, 2008, and 2012. The four organisations concern the ETIM, the Eastern Turkistan Liberation Organization (ETLO), the World Uygur Youth Congress (WUYC), and the East Turkistan Information Centre (ETIC). The 25 designated individuals are all linked to one or more of these organisations. The designation of these persons and entities was prior to the current CTL which now requires FIs and DNFBPs to freeze the assets of these persons or entities. Four accounts have since been frozen, for a total amount of RMB 169.15 (approx. USD 24.82), and the accounts remain frozen while the two account holders remain at large.

251. Since 2012, there have been no domestic designations. The 2016 CTL includes provisions that allow for the designation of terrorists. Designations can be made on an administrative basis by the National Counter Terrorism Leading Body. Requests can be filed by the MPS, the MSS, the MFA, regional/provincial counter-terrorism leading bodies. Courts can also decide to designate a person or entity as terrorists as part of criminal proceedings. As of the time of the onsite, no such designations have taken place. As is the case with proposed designations to the UNSC, this is despite the existence of Chinese nationals fighting in Syria and Iraq as part of ISIL or returning to China from ISIL-held territory. The same applies to persons who have committed terrorist attacks in China in recent years[33] and the support networks of these attackers, also in these cases authorities have not used TFS.

[33] Such as, for example, the 2010 Aksu bombing, the 2011 Kashgar attacks, the 2013 Tiananmen

252. Regarding requests to other countries, authorities indicate that they have requested other countries to designate ETIM as a terrorist organization. Such efforts have been successful in the case of Turkey (2003), the UAE (2014), the U.K. and the U.S. (both 2016). Requests to Australia, Canada, the EU, Germany, and Saudi Arabia did not lead to a designation of ETIM by these states, according to authorities.[34] The authorities explained that these ETIM designation request must be considered as a political statement to signal the importance that China attaches to the fight against ETIM, regardless of the fact that the UNSC since 2002 already requires ETIM assets to be frozen in all UN member states. Despite the risks that China is facing (as described above), no other requests were made by China to other countries.

253. Authorities indicated that the MFA would be responsible for receiving foreign requests to China for designations under UNSCR 1373. According to the authorities, no foreign country has ever made such a request to China.

254. FIs and DNFBPs were generally aware of the domestic lists of designated entities, but not so much in relation to the 4 organizations and 25 persons related to ETIM. Most FIs would refer to the regular, domestic, law-enforcement watch list maintained by the MPS (which for the purposes of the FIs would not make a difference).

255. FIs could not demonstrate an understanding that there is a possibility that the financial infrastructure in one part of the country may be used to finance terrorism elsewhere, or that TF and terrorism could be separated, with terrorist attacks taking place in one place, and the financing of such attacks taking place elsewhere. Rather, FIs expected TF-related transactions to be linked closely to terrorism. This is somewhat of a concern considering that China has large financial centres, both for traditional financial services and for new financial services (e.g., new payment systems, F
this case is actually in line with existing typologies

256. See also IO.4 for more details on compliance of FIs with TFS requirements.

Square attack, the 2014 Kunming train station massacre, 2015 Guangzhou train station attack, and the 2015 Sogan Coal Mine attack.

34 UNSCR 1373 does not require states to positively respond to requests for designation, only to consider these requests.

Targeted Approach, Outreach and Oversight of At-Risk Non-profit Organizations

257. [illegible] 500 social organizations comprised of social groups (368 000), foundations (6 500) and social services institutions (private non-enterprise units) (425 000) as well as 1227 separately regulated overseas nongovernment organizations. The MCA has the responsibility for the registration and oversight of social organizations while the MPS has the responsibility for the registration and oversight of overseas nongovernment organizations. China has failed to date to identify the subset of NPOs that, based on their characteristics and activities, are at risk of terrorist financing abuse as is required under R.8.

258. Since the reform and opening-up in the late 1970s, social organizations have developed rapidly in China. China recognises the positive role social organizations play in promoting economic growth, the development of society, the innovation of social governance, and the deepening of international relations.

259. In 2016, arising from a need to establish a comprehensive legal framework governing the NPO sector, the General Office of the State Council issued the Opinions on Reforming the Administrative System and Promoting the Healthy and Orderly

261. China addresses social organizations in its NRA under Chapter 7 TF Risk Assessment. The analysis,
(social organisations) and the laws and regulations in place to address fund management; responsible person management; activities management; governance, and integrity and self-discipline. There is no analysis as to the types or features of social organizations based on their activities or characteristics that make them vulnerable to TF abuse, neither is there an analysis as to the nature of threats posed by terrorist entities to social organizations or a subset of social organizations or how terrorist actors abuse social organizations. The NRA acknowledges that there are ; however, no cases of NPOs being involved in TF activities were identified.

262. The MCA has the powers to conduct appropriate supervision of social organizations. It has the authority to share information with other government

the AMLJMC. During the NRA process, China assessed the risk of its entire NPO sector, without limiting the assessment to FATF-defined NPOs. While China recognises the inherent risks of TF abuse faced by FATF-defined NPOs, it failed to identify any specific risks of TF abuse faced by NPOs in China. The NRA did however identify ML

China has chosen to incorporate social organizations into its AML regulatory system. While oversight and regulation o
of a concern a ononiaa ingti gya an1n ile (a)cth(l)10 re(a)-204.004m(i)6.005a(fy)0098 (b)3.995e ( )

Consistency of Measures with Overall TF Risk Profile

264. China is a regular victim of terrorism, and Chinese nationals are also active overseas, such as most recently in ISIL controlled territory in Syria and Iraq. ETIM, has been designated by the UNSC under 1267 and successor resolutions. As is described above, for the past years this TF risk profile is not matched by corresponding measures to effectively implement preventive TFS measures. However, the focus of the authorities on criminal measures (convictions and confiscations) does balance this, as is set out comprehensively in relation to IO.9.

Overall Conclusions on Immediate Outcome 10

265.

[illegible]

266. China lacks a comprehensive general legal framework to deal with TFS related to proliferation financing, despite the fact that PBC issued Notice 187/2017 to address some of the shortcomings in relation to FIs. Notwithstanding the legal framework, the overall implementation of targeted financial sanctions related to TF in China suffers from three fundamental deficiencies (as set out below), as well as of a general absence of a focus on UNSCRs related to Iran. These three shortcomings are largely similar to those referred to under IO.10.

- Scope issues and lack of prohibitions: Although Notice 2017/187 contains obligations for FIs to freeze assets of designated entities, China lacks obligations that require all natural and legal persons within the country to freeze without delay and without prior notice, the funds or other assets of designated persons and entities. China also lacks obligations that would prohibit all natural or legal persons to make any funds or assets available to designated entities (i.e., there is no general prohibition). The authorities were unable to demonstrate that these deficiencies in scope do not leave a gap in the effective implementation of DPRK and Iran-related UNSCRs.
- Not all funds, assets and transactions are covered: Because of these scope issues, as a country China is only able to freeze certain assets (e.g., those that would be held by a bank), but is not able to freeze assets that designated persons or entities may be holding themselves, or that other third parties may be holding. In addition, transactions outside the financial sector are not

prohibited. The authorities were unable to demonstrate that these other types of assets (e.g., real estate, land, cash), or other transactions, are effectively frozen or prohibited using other measures. This deficiency impacts the effective implementation of DPRK- and Iran-related UNSCRs as it allows designated entities to move their assets to safety.

- No implementation without delay. Authorities were unable to demonstrate that the freezing actions that the PBC Notice provides for are implemented without delay (i.e., ideally within hours). The initial delays are caused by untimely circulation of new UNSCRs within the government, even before the PBC and others could circulate the UNSCRs to supervised entities.

267. It should be noted that the authorities acknowledged at a high political level the need for China to introduce a comprehensive legal system to deal with targeted financial sanctions related to proliferation financing, and the assessors fully support the authorities in this endeavour.

268. In the absence of a general legal and operational framework for the implementation of the targeted financial sanction provisions of UNSCRs related to the financing of the proliferation of weapons of mass destruction, the PBC has taken steps to implement DPRK-related requirements for the financial sector, most notably through PBC Notice 187/2017 which includes freezing requirements (see also IO.10).[35]

Implementation of Targeted Financial Sanctions Related to Proliferation Financing Without Delay

35 Although not required by R.7, the authorities report that China has taken other measures to reduce the overall risks of proliferation financing. This includes the so-called whole-of-government counter-proliferation mechanism, in which 19 ministries and commissions participate with an aim to effectively control export of sensitive items, in close coordination with the so-called UNSCR implementation mechanism. In addition, the authorities report having taken measures that aim to implement non-TFS related UNSCR provisions. This includes closing banks and other measures to cut financial connections with DPRK; close entities owned or controlled by designated persons; and using criminal measures to suppress violations of the UNSCRs (such as a case of a successful seizure of banned metals by customs). It should also be noted that China has used its mechanism to apply to the UNSC for (de-)listing. For example, in 2016, Chinese MFA successfully applied for the de-listing of several Chinese vessels. Because of the limitations of the FATF standards, these measures have not been assessed or rated in this report.

269. The MFA is responsible for informing other state entities of the existence of new UNSCRs related to PF. Notices consist of a short cover note from the MFA, with a reminder to comply with the requirements, and a copy of the new UNSCR. Authorities shared a few examples of such notices with assessors. PBC is then responsible for communicating the UNSCRs (based on PBC Notice 187/2017), as well as issuing risk alerts to selected FIs. Risk alerts are reminders to FIs but do not impose legal obligations and are not enforceable means and they do not constitute an obligation to freeze the assets of the designated entity.[36]

270. Some or more DPRK-related UNSCRs and two Iran-related UNSCRs were circulated by the MFA to the PBC. It takes the MFA on average slightly over seven days to circulate these to the PBC (and other government entities) after issuing by the UNSC. This is not without delay, as defined by the FATF Glossary (i.e., ideally within hours). It is not clear how long it subsequently takes for these Notices to reach FIs, and it was not demonstrated that amendments to the lists of designated entities are communicated to financial institutions.

271. As is the case with UNSCR 1267 (see IO.10), PBC requires banks to use commercial compliance software to screen for designated persons and entities. This is also done to address the delays in circulation of MFA notices. This is a positive measure, despite the challenges that reliance on commercial software providers can pose. See on this issue also below. Authorities also stated that they consider that the

the biggest banks are state-owned (and therefore should feel compelled to comply). FIs that met with the assessment team generally did not show a well-developed understanding of the requirements of the Notice, or of the UNSCRs, beyond having a high-level awareness of the existence of UN sanctions, and none mentioned that they had identified or frozen assets. FIs also generally were unable to share practical examples of issues that would arise when implementing measures (e.g. updating lists, transliteration issues, incomplete info, similar or identical identifier information).

Identification of Assets and Funds Held by Designated Persons/Entities and Prohibitions

272. To support implementation by banks, PBC has taken additional measures, such as providing training and requiring selected banks to screen their entire

36 450 such alerts are said to have been issued. The one example that was shared contained generic language, reminding banks of the existence of UNSCRs.

database against the UNSCRs. As part of these screening since May 2017 and May 2018, banks identified an undisclosed number of accounts or transactions that may be linked to designated entities related to DPRK UNSCRs (none to Iran). This is evidence that FIs must have some experience in the implementation of Notice 2017/187, despite the lack of feedback given during the on-site (as mentioned above). Such hits include possible false positives and include related transactions and customers (i.e., family members). It is not clear how many of these hits were subsequently confirmed as formal or real hits (i.e., being the assets of the actual person or entity designated by the UNSC). Separately, regarding non-bank FIs and DNFBPs, there was no awareness or experience with the implementation of TFS. No information was provided regarding Iran-related designations.

273. Authorities were able to provide data on the number of accounts frozen by Chinese banks of six entities prior to their designation by the UNSC.[37] Although it is not clear how these assets were identified (e.g., domestic intelligence, foreign requests, by the banks or by authorities), and what the purpose of the freezing action was (e.g., criminal, preventive) these freezing actions do evidence a commitment on the part of the Chinese authorities to act against PF.

274. The UNSC Panel of Experts established pursuant to Resolution 1874 (2009) (hence: DPRK PoE) publishes annual updates on the implementation of DPRK-related sanctions, including the financial provisions of relevant UNSCRs that have been incorporated into the FATF Standards. Based on these updates, it appears that there is room for improvement regarding the identification of assets and funds held by designated persons and entities. The DPRK PoE reports cite examples of accounts, funds or assets held by designated entities in China, and (front) companies run by designated entities in China, some of which acted as de facto banks for the DPRK in China, until detected. The authorities report that the DPRK PoE has send 50 requests to China for information, of which ten requests related to the financial sector, and that China actively cooperates with the PoE. An example of such a request to which China

[37] The names of the entities and the details of the accounts that were frozen were shared with assessors.

responded related to assistance that the DPRK PoE needed in the case of Choi Sam to investigate three companies.[38][39]

• ƒ • † • ï • † ‡ ” • – ƒ • † ‹ • ‰ ‘ ^ ƒ • † ‘ • ’ Ž ‹ ƒ • … ‡ ™ ‹ – Š „ Ž ‹ ‰ ƒ – ‹ ‘ •

275. From discussions with the private sector,[40] only FIs (except for online lending institutions) are aware of the existence of UN sanction regimes. No references were made to the specific domestic legal obligations to freeze assets of designated entities in relation to PF, although in practice this does not seem to matter. FIs would generally make general references to UN-related obligations to freeze assets of designated entities, without distinguishing between TF and PF.

276. The benefits and challenges noted in IO.10 in relation to the use of compliance software to detect funds or assets of designated entities, equally apply to IO.11. The same applies to the FIs understanding of the legal requirements of the legal framework in China or of the UNSCRs, beyond being able to cite the basic legal requirements. As indicated, this is somewhat in contrast to the results of the screening exercises [illegible]

Competent Authorities Ensuring and Monitoring Compliance

277. As indicated, authorities stated that CDD rules (not related to PF) and self imposed rules by FIs robustly prevent the misuse of the financial [illegible]

Key Findings

a) While FIs have a satisfactory understanding of their AML/CFT obligations, they have not developed a sufficient understanding of risks. Measures implemented to mitigate risk are generally not commensurate with different risk situations.

b) The most significant CDD deficiencies relate to ineffective implementation of requirements related to BO and ongoing due diligence. Transaction monitoring by some financial institutions does not focus on assessing whether transactions are in line with the institutions, including some banks, do not systematically refuse business when CDD is deemed incomplete.

c) Measures for identifying foreign PEPs and persons entrusted with a prominent function by an international organization, and establishing their source of wealth, are not effective. Given the significance of corruption in China, the absence of measures applicable to domestic PEPs represents a serious vulnerability.

d) Considering TF risks facing China, the effectiveness of TFS could not be established, including because some FIs do not screen the counterparties to transactions.

e) The types of transactions that are reported are not in line with ML/TF risk profile. The effectiveness of reporting of suspicious transactions is hampered by the insufficient understanding of ML/TF risks, the onerous criteria for determining whether to report an STR or a key STR and the lack of reporting from non-bank FIs. PIs seek to form more than a reasonable suspicion of a predicate crime prior to reporting, which represents a high threshold. Less than 5% of STRs are reported by PIs, while they are identified as having higher-risk of ML/TF in the NRA.

f) Internal controls of Chinese financial groups are often inappropriate for mitigating risks, notably when regulations of host countries prevent access by FIs to information held by foreign branches or majority owned subsidiaries for the purposes of CDD and ML/TF risk management. Considering the importance of foreign branches of Chinese FIs, group wide AML/CFT programs implemented by financial groups have a limited effectiveness.

g) Except for DPMs, DNFBPs are not covered by the AML/CFT framework. DNFBPs have not developed an understanding of ML/TF risks and do not apply preventive measures effectively.

h) Online lending institutions are not covered by the AML/CFT framework and have not developed an understanding of ML/TF risks and do not apply preventive measures effectively.

Recommended Actions

a) Shortcomings in the AML/CFT legal framework related to the coverage of online lending institutions and DNFBPs should be addressed.

b) The robustness of risk assessments of FIs should be enhanced to ensure that these reflect actual threats and corresponding vulnerabilities exposing these institutions to risk. Ongoing due diligence should be strengthened to ensure a better detection of actual threats. These objectives can be achieved through guidance, feedback, and improved typologies.

c) Guidance and training should be provided to FIs and DNFBPs to develop a good understanding of the concept of beneficial ownership and to ensure a systematic rejection of business when CDD is not completed.

d) AML/CFT requirements in relation to domestic PEPs and TFS should be established.

e) The criteria for reporting suspicious transactions under regulatory requirements should be streamlined for all reporting entities, including PIs. Guidance is required to address the inconsistencies of reporting practices by FIs. FIs and DNFBPs should be provided access to reliable, independent identity.

f) Financial groups should (i) apply mitigating measures that are commensurate with the risks of the host country, (iii) strengthen group oversight, including the scrutiny of transactions and the reporting of suspicious transactions, and (iii) inform the PBC of instances of inability to access information held by their branches or subsidiaries.

279. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The recommendations relevant for the assessment of effectiveness under this section are R.9-23.

5.2. Immediate Outcome 4 (Preventive Measures)

Understanding of ML/TF Risks and AML/CFT Obligations

280. Except for online lending institutions, FIs have a satisfactory understanding of their AML/CFT obligations, but an insufficient understanding of ML/TF risks. FIs

generally recognise that there is room for further developing their assessment of ML/TF risks. Banks are far more sophisticated than other institutions in identifying, and to a certain extent, assessing ML/TF risks. Online lending institutions and DNFBPs have not developed an understanding of ML/TF risks or AML/CFT obligations.

281. Most banks identify threats of ML, such as proceeds of illegal fund raising, underground banking, and telecom fraud. This identification is largely derived from the results of the NRA and priorities of regulators and law enforcement authorities. Some banks are more concerned about proceeds of embezzlement, corruption, online gambling, and tax evasion, or POC generated outside China. Information received form supervisors suggests that PIs consider online gambling and pyramid scheme as main ML threats, while some PIs met during the on-site identified illegal fund raising as main threat. Overall, non-bank FIs (including PIs) have a poor identification of threats of ML. In general, FIs did not demonstrate a developed or comprehensive understanding of AML/CFT vulnerabilities, such as determining the aspects of their business that are exposed to these threats and the extent of this exposure. Except for online lending institutions, the threat of TF is commonly identified by FIs; however, the understanding of domestic threats is primarily limited to transactions associated with the Xinjiang province.

282. Banks identify AML/CFT vulnerabilities posed by geography inside China (e.g., Guangdong and Xinjiang provinces; coastal regions in the southeast), or other countries, including those identified for having strategic AML/CFT deficiencies by the FATF. Non-bank FIs generally did not demonstrate such an ability. Except for online lending institutions, most FIs identify non-face-to-face, including online, business as the main vulnerable delivery channels. Banks and some insurance companies identify products/services most vulnerable to ML/TF (e.g., cross-border remittances; e-banking; cash), while the other FIs did not demonstrate such an ability. Most FIs identify only PEPs as a high-risk customer category. Instead, institutions focus on the risk assessment of individual customers, as required by PBC. Some banks, however, have a more comprehensive identification of customer categories that are vulnerable for ML (e.g., small business owners; cash intensive businesses; legal entities) and TF. Only some banks appeared to have developed a certain understanding of these vulnerabilities, especially for products and services, delivery channels, and geography. FIs, especially non-banks, generally have a poor understanding of vulnerabilities posed by the different categories of customers (e.g., legal persons;

non-residents; cash intensive businesses, etc.). Information received from supervisors suggests that insurance and securities companies identify businesses representing higher ML/TF vulnerability (e.g., securities companies identify brokerage and asset management businesses), but it does not amount to an assessment of vulnerability.

283. Except for online lending institutions, most FIs understand their AML/CFT obligations. Some institutions tend to apply standards going beyond domestic requirements, due to the purchase of IT solutions or databases from foreign third-party providers. A few institutions demonstrated confusion regarding some obligations (e.g., reporting of suspicious transactions; due diligence towards domestic PEPs and accounts in anonymous names).

284. DNFBPs relate the lack of understanding of ML/TF risks and AML/CFT obligations to the lack of coverage by the AML/CFT framework. DNFBPs do not have a proper appreciation of the existence and extent of ML/TF risks in China. Some DNFBPs (i.e. lawyers and DPS) consider that the AML Law and some business regulations require the implementation of due diligence, record keeping and the reporting of suspicion; however, the understanding of such requirements is lacking. It was noted that accountants do not perform any of the activities that could subject them to the requirements of FATF standards.

Application of Risk-Mitigating Measures

285. Mitigating measures that are generally applied by FIs are generally not commensurate with their risks. DNFBPs do not apply such measures.

286. Only few banks appeared to have designed and implemented mitigation measures somewhat adapted to the risks (customer risks and, to a lesser extent, the risk of transactions) they identified. These measures are mostly concentrated in the customer identification (e.g., where risks of failure of identification are higher: facial recognition technology) and transaction monitoring (e.g., for overseas ATM withdrawals: monitoring of number of accounts open, identical phone numbers or IP addresses used by multiple customers). However, given the limited understanding of ML/TF risks, these measures are not sufficiently commensurate with the actual risks. Except for online lending institutions, FIs generally assess the risk of customers and implement enhanced due diligence if the risk is high or to address risk warnings issued by the PBC. However, the set of due diligence measures adopted in these cases,

particularly enhanced due diligence, is standard (same measures applying to same customers or transactions assessed to have a particular risk level), applies to different risk situations invariably, and, therefore, is not commensurate with the type and extent of risks. Some FIs (including PIs and online lending institutions) set transaction caps or measures (e.g., business restrictions based on geography) that limit the exposure to risks; however, these measures are not necessarily specific for, or effective in, mitigating ML/TF risks (e.g., limits to credit that are automatically revolving). A few FIs tend to avoid risk by refusing business with certain types of customers or transactions.

287. DNFBPs generally do not apply any risk mitigation measures.

Application of CDD and Record-Keeping Requirements

288. CDD measures applied by FIs are generally not effective. The low level of understanding, identifying and verifying of BO and deficiencies in obtaining BO information represent the most serious deficiency. Customer identification and verification measures and ongoing due diligence are generally performed with limited effectiveness. Record keeping measures are relatively more effective at most FIs. Banks demonstrated a better implementation of these requirements than the other FIs. DNFBPs do not apply CDD and record keeping measures effectively.

289. Most FIs describe a successful implementation of identification measures and verification of identity through the System of Network Check of Citizen Identity Information (SNCCII). However, supervisory findings commonly refer to breaches related to shortcomings in the CDD process, such as incomplete or outdated information on customers, or the expiry of identification documents. Among contributing factors are data limitations of the SNCCII[41], the insufficient access to other reliable, independent source data that can be used for verification purposes, and the inconsistent use of data verification sources mainly by non-bank FIs. There are media reports concerning the frequent utilization of stolen[42] or fake identities, and reports about government initiatives to address such breaches[43]. From March

41 Authorities reported that the SNCCII has a correction mechanism that regularly updates the system for error messages identified, resulting in the coverage of invalid ID information as of April 2018.

42 See www.chinadaily.com.cn/china/2016-05/25/content_25455343.htm

43 See http://news.cnr.cn/native/gd/20170428/t20170428_523731160.shtml .

2018, the PBC began the pilot work of requiring financial institutions to carry out identity verification for invalid IDs,[44] including IDs which were lost or stolen, and IDs which were inconsistent with information of SNCCII. The table below illustrates progress in identification of false ID.

(Unit: Persons or Times

2	

290. Several institutions adopted recognition technologies to mitigate this risk,

challenge for all FIs given the lack of availability of information or data on BO from a reliable source. FIs experience additional difficulties in verifying BO of non-Chinese legal persons. Supervisors stated that they guide institutions to verify BO information through the National Enterprise Credit Information Publicity System and third-party data providers. However, it was not demonstrated that they are reliable sources of information on BO. Online lending institutions do not seek to understand BO.

292. Except for online lending institutions, FIs generally rely on IT solutions for the real-time monitoring of transactions to detect ML/TF unusual transactions. These solutions are developed, or customized to a certain extent, by the institution, and are based on risk indicators that are mostly drawn from PBC risk warnings, and in some cases, were pre-populated by vendors. Except for some banks, most FIs rely on indicators that are generic or not comprehensive enough to detect all unusual transactions. A few institutions (e.g., some securities brokerage institutions) rely on manual or basic solutions for the monitoring of transactions, which does not seem to be commensurate with the volume and risks of their activity. Some institutions (e.g., PIs) do not use information collected under CDD in the monitoring process, in order to understand customers and their business. FIs generally recognise that there is room for further improvement of their ongoing due-diligence systems and processes. Supervisory findings commonly reflect breaches related to the monitoring of suspicious transactions.

293. Except for online lending institutions, most institutions conduct periodic reviews of documents, data and information collected under the CDD process to update it, while only some of these appeared to exert ongoing and effective efforts to maintain documents, data and information up-to-date. However, efforts of most institutions are limited to periodic updating plans, with higher frequency for higher risk clients. Some institutions do not update their records on the occurrence of risk-related events. Supervisory findings commonly reflect breaches related to the updating of documents and data.

294. FIs generally refuse business when CDD is incomplete, with the exception of online lending institutions that do not apply effective CDD. A few institutions, including some banks, do not systematically refuse business when CDD is deemed incomplete, and resort instead to limitations on transactions or postponement of some identification measures with little regard to related risks. A few institutions

(e.g., banks) keep dormant anonymous accounts. These are accounts that existed before the law prohibited anonymous accounts and the institutions have been unable to contact the owners of the accounts to undertake the necessary CDD measures. Institutions reported that they do not allow transactions to be conducted with these accounts.

295. Most FIs apply record-keeping requirements effectively. However, some institutions do not keep records of business correspondence. Supervisory findings occasionally reflect breaches related to record-keeping requirements more generally.

296. DNFBPs do not apply CDD and record-keeping measures effectively. Only some DNFBPs (i.e., lawyers and DPS) apply limited customer-identification and record-keeping requirements for regular business purposes risks; however, the implementation is not effective. DNFBPs generally do not refuse business, except when basic identification measures could not be performed. Most serious deficiencies are the verification of identity (for DNFBPs), due diligence towards beneficial owners, and ongoing due diligence. Record keeping is limited to transaction records and client identity documents.

Application of EDD Measures

297. In general, FIs are moderately effective in applying EDD measures. Measures applied to PEPs are not effective especially considering the significance of corruption. Measures related to correspondent banking relationships, new technologies, and wire transfers are relatively more effective. The implementation of TFS is not effective, especially considering the domestic and external TF risks that China is facing. Measures related to countries with high risk are not commensurate with the risk of business relationships and transactions involving such countries. DNFBPs do not apply EDD measures.

298. Except for online lending institutions, FIs consider PEPs as high-risk customers and rely on third-party databases for the identification of PEPs. Foreign PEPs and persons entrusted with a prominent function by an international organization are subject to enhanced measures. However, only a few banks appeared to have proper risk-management systems to identify customers that are PEPs, such as by ensuring that beneficial owners, family members, and close associates are also identified as PEPs. Other types of FIs relying on third-party databases do not adopt such diligence in identifying PEPs. Some institutions (e.g., some trust management

and securities brokerage institutions) perform a manual screening to determine whether a customer is a PEP or not. FIs do not apply specific measures towards domestic PEP; however, the risk classification of such customers is likely elevated pursuant to identification. Most FIs do not establish the source of wealth and to a certain extent the source of funds, of foreign PEPs and persons entrusted with a prominent function by an international organisation. Few FIs may terminate business relationships with such clients when subsequently identified as PEPs. For some FIs (e.g., some PIs), senior management approval is not necessary to initiate a business relationship with a PEP.

299. Most FIs providing correspondent banking relationships implement specific measures before engaging with respondent banks, such as gathering information on

approval. However, only a few banks appeared to have developed a satisfactory understanding of the nature of the business and the quality of supervision of respondent institutions, including whether it has been subject to ML/TF investigation or regulatory action. Such insufficient understanding of respondent institutions, affects the effectiveness of correspondent institutions in managing risks associated with these relationships that may involve transactions with high-risk countries or countries under UN sanctions. Banks reportedly do not provide services through payable-through accounts and do not establish business relationships with shell banks.

300. FIs, especially payment and online lending institutions, rely extensively on new technologies for the provision of services, mainly in areas of customer identification, channels of delivery, and conduct of transactions. Banks and PIs assess the risk of using new products, practices, and technologies prior to launching. The assessment of such risks by banks covers ML/TF risks and reportedly led in some cases to dropping new products perceived as having an unacceptable risk. Some PIs were sanctioned by the PBC due to the inappropriate management of ML/TF risk of new products, which contributed to notable improvement in risk control measures. For other types of FIs, it is not clear to what extent the risk assessment is performed or covers ML/TF risks. This is an area of concern given the limited understanding of ML/TF risks by these institutions.

301. FIs providing wire transfer services ensure that necessary originator and beneficiary information is included when initiating, forwarding, or receiving a wire

transfer. If a transfer is rejected by the receiving bank due to incomplete information, FIs will seek to complete the information and resend the transfer. Institutions reject wire transfers received if necessary information is lacking. It is not clear how effectively originating banks are implementing this requirement considering the weaknesses in their CDD which are likely to affect the accuracy and veracity of information of originators of transfers.

302. The implementation of TFS by FIs is not effective. Except for online lending institutions, FIs maintain databases of names of persons and entities designated under UNSCRs relating to the prevention and suppression of terrorism and TF. These lists are usually acquired from and updated through third party providers. These institutions also maintain lists of persons related to terrorism offences, provided by the PBC and the MPS. These lists are checked, generally using IT solutions, against names of existing customers and parties to transactions. Due to deficiencies in obtaining BO information most institutions are not in a position to ensure that TFS are applied towards designated persons that are beneficial owners. A few institutions (e.g., some trust management companies) match transactions only at the end of the business day, which would not allow for an effective implementation of possible freezing measures. Mostly banks encountered false positives, but it is not a common practice for these to clear the case through conducting queries with the PBC. However, some institutions, including some banks, reported that no false positives were encountered. Due to the absence of statistics, it was not demonstrated that FIs identify or freeze assets pertaining or destined to designated persons or entities. FIs consider that the deadline for freezing such assets would be 24 hours, should any be identified, but would freeze assets promptly if the hit is positive.

303. Except for online lending institutions, most FIs apply enhanced due diligence towards business relationships and transactions with natural and legal persons from countries for which this is called for by the FATF. These financial institutions maintain list(s) of higher-risk countries that include those for which this is called for by the FATF. Some institutions would also supplement the list with countries they deem to have higher ML or TF risk, spontaneously or based on information on risk disseminated by the PBC. However, a few banks apparently apply a standard set of enhanced due diligence (EDD) measures that is not commensurate with the specific risk of transactions with natural and legal persons from countries for which this is called for by the FATF. (For example, same EDD measures in scrutiny of transactions of domestic customers would also apply to customers from FATF listed

countries, thus no regard to specific country risks). Therefore, given the shortcomings related to enhanced due diligence, it is not likely that applied measures are proportionate to the risks of such business relationships and transactions.

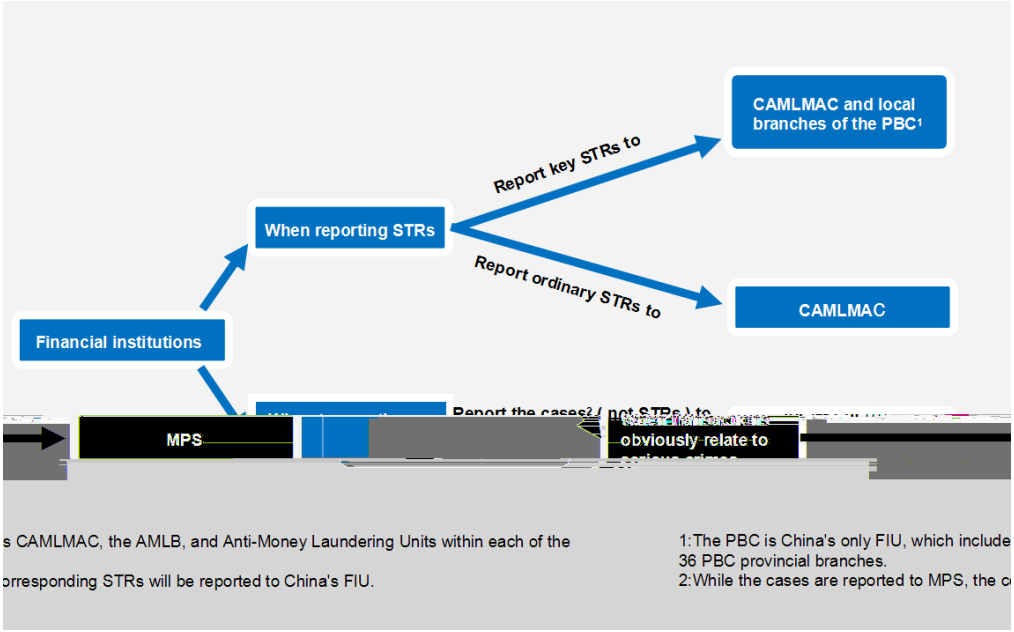
304. Despite ML/TF risks of various components of the DNFBP sector, the latter do not apply EDD measures. This is mainly due to the lack of understanding of risks and the lack of legal AML/CFT requirements.

Reporting Obligations and Tipping Off

305. In general, FIs are moderately effective in reporting suspicious transactions. There are inconsistent practices of reporting, some of which could potentially trigger tipping-off (see further below). Types of proceeds reported in STRs seem inconsistent with the risk environment and are concentrated in the banking sector; the number of STRs reported appears to be modest, considering the size of the financial sector in China. The reporting of suspicious transactions by DNFBPs is very rare: only six STRs submitted so far.

306. FIs report to CAMLMAC funds that are suspected to be the proceeds of a criminal activity or are related to TF. For transactions where ML/TF conduct is obvious,[45]
related to terrorism or TF or conduct affecting national security, institutions report (as required) key STRs,[46] mostly in writing to PBC branches. The same information is simultaneously reported to CAMLMAC. Some financial institutions experience challenges in determining whether a case should be reported as an STR or key STR. If no predicate offence is identified, some institutions would report STRs to CAMLMAC, while others would report the case to MPS without submitting an STR to CAMLMAC. Some institutions (e.g., some banks) also send reports on suspicions simultaneously to the local PBC branch and MPS. Therefore, reporting practices are not consistent across all FIs. However, authorities explained the reporting process (see figure below) and stated that FIs would report to MPS (with corresponding STRs sent to the

45 See TC Annex c.20.1.
46 See analysis under IO.6 and TC Annex, c.20.1.



307. The reporting of suspicious transactions is not done promptly. For non-obvious ML/TF conduct, an average of 10-15 days elapse between the discovery of an unusual transaction and the reporting of suspicion by FIs (mainly banks), if any. During this time, the FI consults and updates as necessary CDD information, and conducts further analysis to confirm suspicion. However, once a suspicion is formed, most FIs consider that the deadline for reporting suspicion is five business days (ten days for PIs); therefore, the practice tends to be the reporting within five days Measures for the Administration of Financial Institutions' Reporting of Large-Value Transactions and Suspicious Transactions FIs to submit an STR promptly, which is specified to be no later than five working days. The articulation of five working days is inconsistent with the notion of promptly and constitutes a technical deficiency which has been addressed by a regulatory update at the end of the on-site visit.

308. As indicated in IO.6, CAMLMAC and the PBC provincial branches have worked with FIs since 2012 to reduce the volume of defensive reporting and improve the quality of STRs and key STRs. The number of STRs decreased significantly against an increase in key STRs. Overall, the quality of key STRs is higher than the quality of STRs because financial institutions conduct a more in-depth analysis to identify a predicate offence in view of reporting a key STR. According to the PBC, a high percentage of key

[47] which are disseminated to LEAs. Therefore, key STRs are generally good quality reports, while STRs have less in-depth analysis impacting their quality.

309. Banks report more than 95% of STRs and key STRs (the majority of the other reports are made by PIs). The structure of reporting by type of institution is therefore inconsistent with the ML/TF risks of sectors, such as PIs and online lending institutions assessed to have high ML/TF residual risks in the NRA, and life insurance institutions assessed to have medium ML/TF risks. Online lending institutions, which are not subject to AML/CFT supervision,[48] did not report suspicious transactions. There is also a concentration of reporting by a number of FIs under each category (see tables below).

[49]

47 See analysis under IO.9.
48 See analysis under IO.3.
49 Trust companies, financial asset management companies, finance companies, financial leasing companies, auto finance companies and money brokerage companies.

310. Considering the size of the financial sector in China, and the size, intensity of activity and ML/TF risks of some sectors, the overall number of STRs appears to be modest, yet decreasing in the banking and insurance sectors (see first table above). One of the contributing factors could be the insufficient understanding of ML/TF risks and the demanding criteria for reporting suspicious transactions, requiring the determination whether an STR or a Key STR should be filed. FIs only report a key STR to a PBC provincial branch and CAMLMAC when they are able to identify an underlying predicate offence, otherwise, they would file a whistle blower report directly with LEAs without filing an STR or key STR in parallel.[50] Therefore, there clearly exists a need for guiding reporting entities to address the ambiguity in the reporting requirements as to whether to file an STR or a key STR. As for PIs, more than a reasonable suspicion of a predicate crime should be formed prior to reporting, which represents a high threshold of suspicion.[51] These practices could explain the quick drop in the number of STRs and the increase the number of key STRs since 2012, thus affecting the effectiveness of reporting by FIs. Supervisory findings commonly reflect breaches related to the reporting of suspicious transactions.

311. The authorities submitted information related to key STRs but could not submit information on the nature of predicate offences related to reported STRs. However, most FIU disseminations[52] 2016 re

[53] (50%), terrorism (15%), financial fraud (8%), drug crimes (4%), and corruption and bribery (2%). FIs apparently have a better ability in identifying transactions associated with terrorism than with TF. As a very limited

50 See analysis under IO.6.

51 See analysis under R.20 in the TCA below.

52 oactive Disseminations (by Types of Crimes).

53 Includes the crimes of: illegal absorption (including in disguised form) of public deposits, forging or altering financial bills, relending loan currency to others at a high interest rate, evading the state control of foreign exchange and ML.

number of institutions report suspicious transactions on TF (see table below) especially in the banking and PI sectors where TF risks are classified as high. China could not demonstrate the effectiveness of reporting of suspicion TF. Except for on-line lending institutions, FIs report attempted transactions involving suspicion; however, it is not clear to what extent this practice is consistently applied.

312. The practices of some institutions when reporting suspicious transactions appear to involve risks of tipping-off. Some FIs (e.g., some PIs) reportedly freeze transactions with customers upon reporting suspicious transactions without informing

inappropriate for mitigating risks, especially when regulations of host country prevent access to information.

315. Except for online lending institutions, FIs implement programs against ML/TF and have compliance arrangements in place; however, the effectiveness of these programs is often questionable. Although institutions developed policies and procedures, these are not designed or implemented on a risk-sensitive basis, as elaborated above. Institutions sanction staff who commit financial crimes (e.g., fraud); however, most institutions do not sanction staff for breaching AML/CFT policies and procedures. Training programs are frequently implemented by most institutions, and cover all staff with AML/CFT responsibilities, including senior management. However, training programs of some institutions (e.g., some banks) do not effectively include senior management, including directors of the Board, (see table below: compare attendance of senior management with number of training sessions), and are not sufficiently sophisticated to improve the skills of staff with key AML/CFT responsibilities. Some FIs, including banks, consider that they could benefit from further investment in resources to improve the capacity of staff and senior management. Audit findings generally do not cover important shortcomings identified by supervisors, such as the monitoring and reporting of suspicious transactions. For many institutions, including banks, the reporting of AML/CFT issues to the senior management focuses on regular compliance issues and individual cases of suspicion. More general risk management issues identified by compliance management are not consistently reported to the senior management.

316. Foreign branches and majority-owned subsidiaries of Chinese banks are significantly relevant to the financial system.[54] The effectiveness of group-wide AML/CFT programs implemented by financial groups is limited. Groups have

54 See info under Chapter 1.

compliance and audit functions at the group level. Requirements for branches and majority-owned subsidiaries appear to mirror those applicable in China, except for host countries with stricter requirements. However, the monitoring of transactions and the management of risks of these branches and subsidiaries does not seem to be sufficiently effective. Group oversight functions, sometimes, do not proactively identify, request information on, nor analyse unusual transactions or questionable risk management practices. A number of institutions reported their inability to access information held by their branches or subsidiaries in some countries due to data protection rules. PBC statistics indicate that, on average, nearly 50 Chinese financial groups experienced issues in accessing information held by their foreign branches and majority-owned subsidiaries in recent years. Most of these institutions stated that issues of access to information are resolved by conducting onsite visits, and some did not take actions to address these issues. In such circumstances, financial groups do not seem to apply appropriate additional measures to manage the ML/TF risks, and do not inform home supervisors. Sanctions applied by foreign regulators on branches and majority-owned subsidiaries operating abroad (including for failure to identify and report obvious suspicious transactions, and, in one case, for tipping off concerned customers) suggest that group-wide AML/CFT programmes of some financial groups do not ensure that stricter standards are implemented when there are jurisdictional STR reporting differences, and are therefore not effective in managing ML/TF risks.

317. DNFBPs do not implement programs against ML/TF. This is mainly due to the lack of regulatory requirements.

Overall Conclusions on IO.4

318.

Key Findings

a)

Recommended Actions

a) Supervisory resources at the PBC should be reviewed to address the need for increasing on-site inspections in the banking sector, adequate supervision of the DNFBP sectors, and the extension of the AML Law to the online lending sector.

b) The PBC should review the balance of resources applied to inspections of high-risk financial institutions by increasing the frequency of inspections of high-risk banks to address the growth in this segment of the supervised population.

c) The PBC and other financial sector supervisors should ensure there is a consistent application of supervisory processes to focus on effective risk-based implementation of internal controls applicable to or supportive of AML/CFT obligations.

d) China should extend the AML Law to cover the online lending sector and ensure effective AML/CFT supervision by the PBC.

e) China should demonstrate collaboration with the relevant DNFBP sector regulators/SROs in designating the DNFBPs that will be subject to the AML Law. It could also consider amending this requirement of the AML Law to give sector regulators a supportive role similar to that of the sector financial regulators.

f) China should conduct a risk assessment of individual DNFBPs as defined by the FATF (apart from trust companies and DPMs) to ensure that (i) appropriate market entry and preventive measures are established, and (ii) the PBC can supervise and monitor appropriate AML/CFT obligations. In doing so, China should review the strategy and necessity of collaborating with sector supervisors in the DNFBP sectors, given their low level of knowledge about ML/TF risks.

g) China should review the effectiveness, proportionality, and dissuasiveness of financial sanctions, and consider substantially increasing the size of penalties for violations of the AML Law, especially for penalties levied against the largest FIs by PBC for violations of the AML Law or by sector supervisors for system weaknesses across financial groups.

h) China should prepare guidance directed at the DNFBP sectors to assist them in implementing AML/CFT measures when they become formally designated as DNFBPs.

319. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The recommendations relevant for the assessment of effectiveness under this section are R.26 - 28, R.34 and 35.

Introduction

320. The AML Law (Arts. 4 and 36) provides inter alia that the PBC is in charge of AML/CFT supervision and administration throughout China. In the financial sector, its work is supported by the sector financial regulators, and in the DNFBP sector, it is required to supervise in collaboration with sector regulators.

321. There is a large on-line lending sector which is subject to high level AML/CFT obligations. While PBC is the designated supervisor for this sector, the sector is not yet subject to any AML/CFT supervision.

322. Generally, PBC treats PIs as FIs but as noted above PIs are not supervised by the sector financial regulators; their AML/CFT supervisor is PBC.

323. The financial sector supervisors have a defined AML/CFT supporting supervisory role (See TC analysis) that is foc
Financial sector supervisors cannot impose sanctions against FIs for AML/CFT violations under the AML Law, and can only impose sanctions against FIs on the implementation of internal controls required by sector legislation.

324. For DNFBPs, the AML Law requires the PBC to designate the DNFBP sectors that are subject to the AML Law and AML/CFT supervision collaboratively with each . At the time of the on-site visit, these were the MOHURD for the real-estate sector; the MOJ for the lawyers sector; the MOF for the accounting sector; and the SGE (which is supervised by the PBC) which is an SRO for DPMs. As with the financial sector, DNFBP sector supervisors and SROs cannot impose sanctions against FIs for AML/CFT violations under the AML Law.

325. For more than 10 years, the authorities have had ongoing discussions with DNFBP sectors and some sector supervisors about designated AML/CFT coverage and supervision. The NRA confirms that the DNFBPs have not yet constructed effective CFT working systems and that the specific coverage of DNFBPs in China is not clear. China has not yet designated AML/CFT obligated DNFBPs, which is required in the AML Law Detailed CFT obligation requirements for DNFBPs have not been issued; neither are there detailed requirements specific to DNFBPs on customer

identification, due diligence, or transaction reports. Overall, there is a lack of relevant regulation and guidance for CFT measures in DNFBPs.

326. During the on-site visit the PBC, as authorised by the AML Law, purported to designate the categories of DNFBPs that are subject to AML/CFT obligations in China (except for trustee services, which are provided by trust companies regulated as FIs in China, and DPMs see TC analysis). Authorities could not demonstrate effective collaboration between the PBC and the DNFBP sector supervisors as part of the required process of purported designation and have therefore not accepted the designation as being compliant with the AML Law and thus not in effect

327. The purported designation Notice named CSPs as a DNFBP sector, despite the information in the NRA precluding the existence of, and a risk assessment of, the CSP sector. The NRA states that there is no CSP sector in China despite instances of the use of CSPs by illicit actors, of which China is aware. During the on-site visit, the authorities advised the assessors that the CSP sector in China engages in agency services such as business registration and consulting services, which according to the authoriti
not share this view based not only on their understanding of the FATF definition but also on several interviews conducted with CSPs during the on
view is that company formation services, including the provision of business addresses, correspondence and administrative addresses for legal persons, are offered by CSPs in China.

normally provided by MPS. As noted in the TCA, there is a minimum period of between three to five years to be covered in criminal checks, depending on the sector. However, in practice, the authorities screen all applications through the criminal databases with no time limit, and thus the authorities can obtain any applicable criminal background information as of the date of the data request.

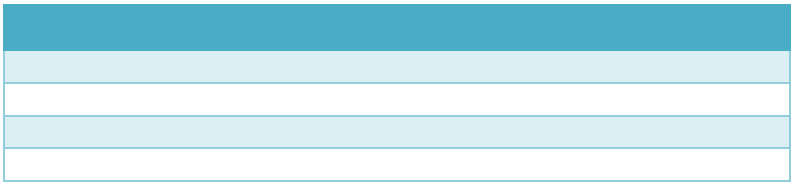
330. The following tables set out statistics about the fit and proper process applied by the authorities in the financial sector between 2015 and 2018.

Table notes:

1. The Securities dealer figures exclude statistics on futures companies. During the period, there were no applications for the establishment of futures companies and there was one license revocation (not for criminally connected reasons).

2. Data as of the end of 2017

the same holding group; the licenses of 16 PIs with serious violations were not renewed, and the licenses of 6 were revoked. The following table provides a further breakdown of the types of PI licensed in China.



333. The regulations governing online lending institutions appear to focus on defining the sector in terms of person-to-person (individuals lending to other individuals) and companies. The banking regulator has issued general (not AML)

seems tobe ensuring that operators do not conduct unauthorised business such as fund pooling or other illegal activity.

336. In summary, there are a few shortcomings in the fit and proper TC framework in most of the regulated FI subsectors (see TC analysis), mostly relating to the minimum periods of time applicable to criminal background checks, but in practice criminal records are accessed by the authorities in processing fit and proper applications. There are no measures applying criminal background checks by the provincial authorities in the online lending sector. In the DNFBP sector, the real estate, DPS and CSP sectors are not subject to entry or ongoing criminal background checks, and the scope of checks by sector authorities is not clear in the legal and DPM sectors.

— ' ‡ ” ˜ ‹ Understanding and Identification of ML/TF risks

Financial Sector

337. The PBC imposes obligations on FIs to conduct inherent risk assessments (Measures for the Anti-Money Laundering Supervision and Administration of Financial Institutions (For Trial Implementation)), to update this assessment annually and provide information to the PBC. The PBC has issued rules and guidance to FIs on the model to use to measure inherent risks, and controls. The PBC uses this information as the starting point for its own risk analysis. These measures establish a system of rating the residual ML/TF risk levels in FIs by assessing the identified inherent ML/TF risks and the strengths of the control measures implemented by FIs to mitigate those risks. The rating for each FI determines the overall level of residual risk, which is used to prioritise supervisory measures.

338.n

fall into prescribed categories based on size thresholds and products. FIs are required to classify clients as high risk under certain specified circumstances. The Guidelines do not apply to the online lending sector as they are not subject to PBC supervision.

339. Risk classifications by FIs are subject to review by the PBC, but the extent to which the PBC applies directions where they believe institutions have not assessed risks accurately is not clear. The PBC provided a number of case studies demonstrating how this process works in practice and illustrating examples of directions to change risk assessments to take into account inherent risks based on known cases of abuse.

340. There are 20 prescribed ML/TF risk control factors, that address the comprehensiveness of systems, rationality of mechanisms, technical support capability, staffing, customer identification, specific measures for high-risk customers, preservation of customer identity information and transaction records, large-value and suspicious transaction reports, measures regarding high risk businesses, AML/CFT training and publicity, internal audit and management.

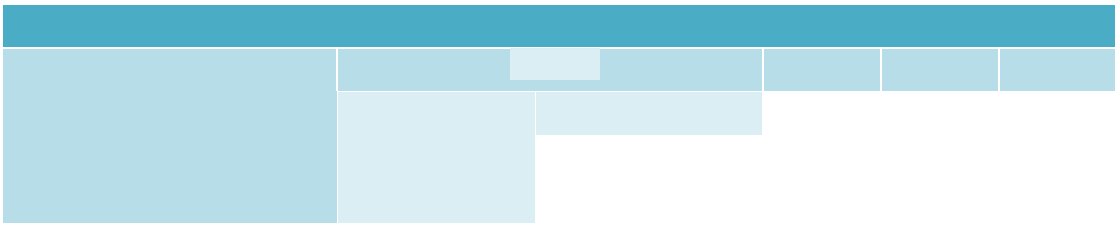
341. The PBC conducts research on the vulnerabilities of financial institutions, particularly in their development of new products and services, and use of new delivery channels. In 2017, nine research papers on new delivery channels and six on new businesses were produced. The financial sector in particular, including PIs, has been developing financial products such as payment systems using internet-based technology. This research feeds into the risk assessment model, which in turn is periodically updated.

342. Although the PBC has not developed a comprehensive supervisory strategy to address these trends, it deals with ML/TF threats associated with potential vulnerabilities by issuing Notices and Risk Warnings, notably in 2016 and 2017, on such topics as bank card fraud through self-service machines, card-free deposits and associated TF risk, and suspicious indicators concerning cross-border transfers. It has also issued a Notice about the risks of dealing in crypto currencies. The National Internet Finance Association of China issued a series of Risk Warnings about Fintech products, including Initial Coin Offerings (ICOs), crypto currencies, and small loans. As can be seen, these measures generally address threats relating to the use of technology to commit predicate offences, rather than vulnerability to ML/TF, and thus the impact of these Notices and Risk Warnings on the risk assessment of financial institutions is not clear.

343. The PBC also receives other information on FIs and PIs from STR data provided by CAMLMAC; criminal case convictions from the SPC; criminal investigation data provided by the MPS; and typological cases provided by LEAs at the national and local levels. However, this process does not address the low level of understanding of risks as identified in Chapter 2. Nevertheless, as a result of these efforts, there has been a significant increase in the numbers of FIs designated as high risk which has implications for supervisory resources (see Risk-Based Supervision of Compliance with AML/CFT Requirements, below).

344. The information obtained by the PBC from sector regulators on internal controls varies in utility and content. Except for the information from the insurance sector, internal control information from the sector supervisors is not AML/CFT-specific and essentially confirms that controls are in place, or otherwise. As noted the PBC itself assesses the overall quality of AML/CFT controls in FIs and PIs.

345. classification of residual risk rankings for the years indicated.



DNFBP Sector

347. The PBC has not conducted any risk assessment of individual DNFBPs (aside from trust companies). The only information available on sector risk is contained in the NRA, which rates the real estate sector as having relatively high inherent risk and medium residual risk.

348. In the NRA, the DPM sector is rated as having relatively high inherent and residual risk, thus implying the risk mitigation is essentially ineffectual. The legal, notarial and accounting sectors are rated as having low inherent and residual risk. The CSP and DPS sectors are not discussed in the NRA and are unrated.

349. The DNFBP sector supervisors (the MOHURD, the MOF, and the MOJ) demonstrated a low level of understanding of ML/TF risk. The authorities stated that the sector supervisors are actively involved in the ML/TF risk assessment process, but no specific or detailed information was provided to demonstrate this. During meetings with DNFBP sector supervisors, the PBC responded to most of the questions about the work done to date on planning for supervision in these sectors.

Risk-Based Supervision of Compliance with AML/CFT Requirements

Financial Sector

350. The AMLB, from its headquarters in Beijing and through 36 locations across

352.
assessment process described under
of ML/TF Risks, above, which results in a AML/CFT supervisory rating.

353. The PBC offices are staffed according to the numbers of prefectures, provinces or counties for which they provide supervisory services, and this allocation does not always correspond to the numbers of financial institutions in these regions. However, the PBC actively manages the assignment of AML supervisors to the locations needing them. For example, the Shanghai branch, which is responsible for one of the largest financial centres in the country, only has 11 staff dedicated to AML/CFT supervision physically located in Shanghai. However, PBC actively assigns additional resources to Shanghai when needed (see further discussion below). Generally, the number of PBC supervisory staff is slightly higher in the four SE provinces of China, roughly corresponding to the areas of higher risk noted in the NRA. The proportion of staff per province is about 12% on average, compared to nearly 13.5% in the SE region.

354.
control processes at FIs. However, the dividing line between PBC and sector supervisory work is not always clear in practice, with supervisors confirming to the assessors that there are often situations where supervisory work plans overlap. This is most notable in the insurance sector (see below and also previous section on risk assessment process). The authorities consider that, given the importance of internal controls, it is important that sector supervisors work cooperatively with the PBC where necessary to ensure internal controls are adequate. The assessors note that the support of the sector supervisors in assessing the quality of internal controls is a strength of the system.

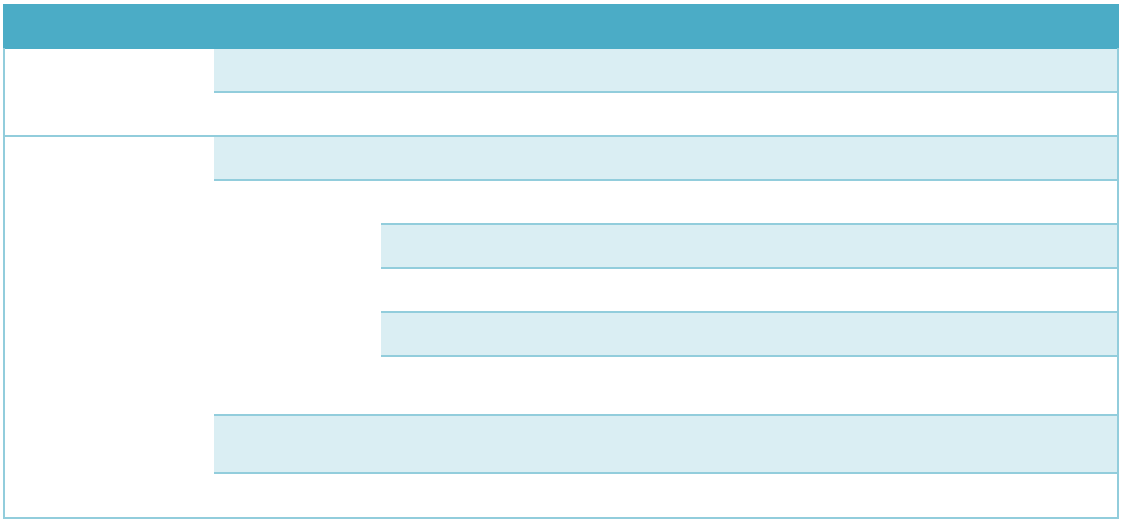
355.
systems of insurance companies. These inspections are not limited to internal controls but cover such elements as customer identification obligations and not reporting LVTRs and STRs, areas that mostly fall to the PBC to supervise in the other sectors. The supervisory programme of the insurance regulator is thus more attuned to ML/TF risks than those of the other financial sector regulators. The banking and securities regulators do not have a comparable approach except where the PBC requests their assistance or input. The assessors consider that similar programs of enhanced support by the banking and securities regulators would further enhance the quality of AM/CFT supervisory process in the financial sector.

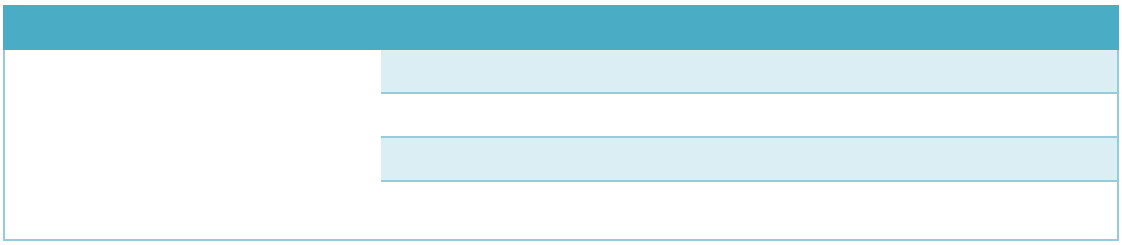
356. The PBC on-site process has two components: supervisory visits and onsite inspections. See Table below for statistics on these two different measures between 2015 and 2017.

357. PBC Supervisory Visits: these are widely used and normally result in obtaining information through questionnaires, information checking, systems inspections, and so on. The supervisory visit is essentially a lighter touch type of supervision used at FIs with lower than the maximum level of assessed risk, and at other FIs to address particular issues. The PBC uses information gathered to document AML/CFT issues and inform the issuance of guidance (see Promoting by Supervisors a Clear Understanding of AML/CFT Obligations and ML/TF Risks, below). Supervisory visits do not normally result in written findings or remedial measures directed at individual FIs. In 2017, the PBC conducted almost 7500 supervisory visits to the head offices of 4000+ FIs and issued a total of 4121 Regulatory Opinions after these visits.

358. On-site Inspections: The PBC AMLB, through the HO and 36 branches, plan annual programs of onsite inspections taking into account supervisory goals, ratings, risk assessments, regulatory filings, and risk events (known instances of higher risk) during the planning process. The chief criterion is the risk rating. The principal objects of the onsite inspections are to verify that the FI has implemented customer identification, record keeping, monitoring, STR filing, and TFS name scrubbing processes.

(Number of Institutions)





359. Given the significance of ML threats arising from cross-border transfers and the NRA rating of the banking sector as high inherent risk, the inspection statistics in the table above indicate that the banking sector appears to be substantially under-

unts for a significant number of inspections. As shown in this table, the ratio of inspections to the numbers of high-risk banks has declined somewhat, from approximately 50% in 2015 to 47% in 2017. On the other hand, in the PI sector this ratio has improved from 9% to 31% over the same period.

360. In the securities and insurance sectors, the numbers of inspections exceeded the numbers of high-risk FIs, which suggests the PBC includes a higher proportion of medium and low risk entities in the inspection programs in these sectors. Generally, it is not clear what proportion of inspections in each sector apply to high-risk entities, but it appears there is an imbalance in these sectors which should be addressed.

361. The PBC does not carry out on-site inspections at foreign branches or subsidiary locations of Chinese FIs. The authorities explained that (i) these foreign locations account for less than 2% of all FI locations and about 12% of total assets; (ii) FIs are required to report to the PBC on the AML programs at these locations in their annual reporting to the PBC; and (iii) FIs are required to report to the PBC on

adequate to assess the risks emanating from foreign locations.

362. During on-

risks associated with FinTech products, including whether new FinTech products have been subject to a risk assessment prior to being launched, and they assess the effectiveness of this process. This is a useful process, but it would be more beneficial if the PBC also made these risk assessments following the on-site supervisory visits. This would allow the PBC to study the risk management practices adopted for these products across the financial sector, would improve the quality of information available as the PBC prioritises FIs for supervisory activity.

DNFBP Sector

363. The PBC, accompanied by the MOHURD, the MOF, and the MOJ, have carried out a small number (53) of supervisory visits (not inspections) to DNFBPs [as defined by the FATF standards] in the real estate, accounting, legal, notarial and DPS sectors from May 2017 to June 2018. A further 105 supervisory visits were made to various other firms, mostly tax firms and pawnbrokers. It is worth noting that none of these other types of firms was included in the purported July 2018 designation of DNFBPs referred to above. The objectives of these visits were mainly to acquaint industry participants with potential AML/CFT obligations and possible proposals for future supervision, as part of the process of discussing future supervision with the sector

ators were in a position to enforce AML/CFT obligations before the purported July 2018 Notice was issued.

364.
established AML internal control frameworks and set up reporting procedures to process STRs and LVTRs. Again, however, it is not clear how these internal controls and procedures could be evaluated given the lack of enforceable measures in the sector. The competent authorities did not provide any statistics on these control frameworks or processes, or which DNFBPs had established them. Accordingly, the assessors conclude that there has been no AML/CFT inspection of the DNFBP sectors (aside from trust companies and the DPM).

365. In summary, although the concept of risk-based supervision seems to be understood by the PBC, the extent of its understanding of ML/TF risks (see

allocation of inspection resources is entirely aimed at the financial sector and is predo own risk assessments and a process that assesses the general quality of internal control measures. Moreover, the growth in numbers of high risk FIs is outpacing the efforts of the PBC to inspect these FIs. DNFBP supervision for AML/CFT obligations was essentially non-existent since measures did not apply to these sectors (aside from trust companies and DPMs). As a result, the adequacy of the overall results of the supervisory process in mitigating the ML/TF risks in China is questionable.

Remedial Actions and Effective, Proportionate, and Dissuasive Sanctions

366. PBC and the sector regulators have a range of supervisory remedial measures and financial sanctions available for the financial sector.

367. Remedial Measures: The — ’ ‡ ” ˜ ‹ • ‘ ” › ’ ‹ following supervisory visits, setting out identified issues and requiring the financial sector to implement within a specified time limit. Following inspection visits, individual FIs are required to develop specific remediation plans, implement the plans, and improve AML/CFT work in aspect of organisational structure, investment of resources, internal control mechanisms, and system improvements. The PBC regularly reviews the status of remediation, hears reports from the senior executives, and guides the follow-up work. If the FI fails to comply by the deadline, more intensive measures and/or financial sanctions are available. Remedial measures, when completed, must be reported to the supervisor. Progress (or lack of it) is a factor in the ratings system described above and in supervisory strategy going forward. Remedial measures applied by PBC are always accompanied by a financial penalty.

368. Financial Sanctions: Financial penalties available to PBC for violations of the AML Law are as set out in the TCA
According to the authorities, the amount of the assessed penalty is based on the number and degree of severity of violations. China also follows a policy of assessing additional financial penalties against members of the boards of directors or senior management considered responsible for the violations of the FI legal entities.

369. The table below sets out statistics on the numbers of FIs and related individuals that were subject to financial sanctions applied by the PBC in the years indicated.

370. Banks penalized by the PBC under the AML Law represented about 6% of all banks in China in 2017. In 2017, of the 255 FIs that were financially penalized, 157

were mostly residually high-risk small- and medium-sized urban commercial banks, rural commercial banks, rural credit cooperatives and rural banks. Although these banks offer services assessed as relatively high risk by the NRA, their smaller scale of business coupled with weaker controls makes them residually higher risk. As a result, more issues were identified in on-site inspections, and thus the proportion of penalties was higher. In 2017, the penalized number of such banking institutions amounted to 61% of the banking sector and the aggregate penalties amounted to 57% of all penalties in the sector.

371. For 2016 and 2017, China applied an aggregate of RMB 48.7 million in financial penalties to 19 out of the 24 FIs directly supervised by PBC HO, or an average of about RMB 2.6 million each. The largest penalty (RMB 7.9 million) was applied to the largest bank in China for infractions found at 26 locations. As of the end of June assets were RMB 8.5 trillion, total deposit balances were RMB 7.8 trillion and total loans portfolio amounted to RMB 3.3 trillion. This size of penalty applied to such a large bank for extensive systemic violations at 26 offices seems minor and not dissuasive.

372. As noted above, the sector financial supervisors cannot apply financial penalties for violations of the AML Law but can apply sector penalties for weaknesses in internal controls. According to available statistics, since 2015, the former CBRC has imposed 48 penalties and fined financial institutions an aggregate of RMB 22.3 million for failure to implement internal control requirements. A total of 23 institutions were penalized, 6 were also ordered to sanction 25 responsible personnel of whom 8 were removed from their posts and 3 were prohibited from engaging in the banking industry for life. The average penalty per FI was slightly less than RMB 1 million (approx. USD160 000). Again, in a sector which features very large banks, this average size of penalty seems minor and not dissuasive. No information is available on the relative level of ML/TF risk in these FIs.

373. The CIRC applied financial penalties to two insurance companies in 2017, but the amounts and violations were not available. In 2016, CSRC imposed administrative penalties on four institutions aggregating RMB 240 million.

374. As can be seen from the table above, the overall volume of financial penalties applied by the PBC is growing. The authorities attribute this growth to the impact of new regulatory obligations, better targeting of inspections to higher-risk entities and better inspection methodology leading to more issues being identified by PBC.

However, the low levels of penalties available (see TC Analysis) means that in order to have dissuasiveness keep pace with growth in risk levels, the supervisory have to expand the scope of their work in order to find violations that will generate a sufficiently large penalty.

375. In summary, the assessors believe that AML/CFT financial penalties available, as applied by PBC and averaging about RMB 41 million per year (approx. USD million) are not effective, dissuasive, nor proportionate given the overall size of the financial sector, the scale of the major banks and other FIs in the financial sector, and the lack of initial responses to remedial measures. Further, although the sector supervisors can and do apply sector financial penalties for internal control weaknesses, these penalties are not necessarily AML/CFT-related and apply for broader issues that may or may not have a direct link to AML/CFT compliance.

376. No AML/CFT remedial actions or sanctions have been applied to online lending institutions.

DNFBPs

377. No AML/CFT remedial actions or sanctions have been applied to DNFBPs.

Impact of Supervisory Actions on Compliance

378. The PBC demonstrated that its risk-based approach to AML/CFT supervision

ntrols applicable to implementing AML/CFT measures. The overall impact of supervision on compliance by the financial sector seems to be moderate and declining. This conclusion is based on the following factors: (i) the rapid growth in the number of high-risk FIs which is outpacing increases in numbers of inspections; (ii) increasing remedial measures required of, and financial penalties handed out to, FIs and individuals in the financial sector between 2012 and 2017; (iii) the lack of dissuasiveness of financial penalties as discussed above; (vi) the low to moderate level of ML/TF risk understanding demonstrated by the financial sector during the on-site visit (see Preventive Measures); and (v) the lack of AML/CFT sanctions in the DNFBP sector.

379. For example, between 2012 and 2017 the number of FIs that were sanctioned by the PBC for violations of the AML Law grew from 83 in 2012 to 429 in 2017, over a 400% increase. Over the same period, the number of on-site inspection

from 1 173 to 1 046, a reduction of about 11%. In 2012, 32 individuals in these institutions were fined, and this number grew to 695 by 2017. The aggregated amounts of annual fines grew from RMB 13 million in 2012 to RMB 107 million in 2017.

380. Sector Supervisors: Except for the insurance supervisor, the sector supervisors have a low to moderate impact on AML/CFT compliance, due to their supporting role that is limited to verifying the existence of general internal controls and their inability to apply financial sanctions for AML/CFT violations. Their

oriented to prudential supervision. The insurance supervisor carries out its own assessment of internal controls relevant to ML/TF in insurance companies. The

cannot apply financial penalties for AML/CFT deficiencies, and remedial measures applied were negligible and not directly related to supporting AML/CFT controls.

381. Despite the increasing use of financial penalties, the overall levels of compliance behavior by FIs have not changed significantly and in some respects has worsened. For example, there has been steady growth in the number of sanctions for issues relating to BO, growing from 57 in 2015 to 119 in 2017. The authorities attribute most of this increase to non-compliance issues relating to the identification of beneficial owners, introduced under Regulation 235 in 2017.

382. Since 2015, the 22 largest FIs in China (including the two largest PIs) had spent in excess of RMB 30 billion on human resources, systems, training and other services to improve their AML/CFT controls as a direct result of remedial actions taken by PBC.

383. The following table sets out statistics on deficiencies identified by PBC related to weaknesses in management of ML/TF risks associated with FinTech products in AML inspections from 2015 to 2018. As can be seen there has been a steady decline in the number of issues, suggesting that the impact o
sector relating to FinTech products has achieved positive results.

384. Online lending sector: PBC and the financial sector regulators have no impact on the online lending sector as these entities are only subject to local municipal registration and not to AML/CFT supervision by PBC. The online lending sector

notwithstanding that the AML Law does not apply to online lenders. Despite this, however, no inspections in this sector have been conducted by PBC (see above Table on Statistics of Various Supervision Measures Conducted at FIs by the PBC).

DNFBPs

385. PBC and sector regulators/SROs had little to no impact on compliance by DNFBPs. The authorities asserted to the assessors that in practice, the PBC collaborated with sector regulators to conduct AML/CFT supervision on DNFBPs in the real estate, DPM, and accountant sectors through issuing various Notices. These Notices simply highlighted high-level expectations but did not apply the AML Law to these sectors. As noted above, by June 2018 the PBC had carried out supervisory visits (which do not result in remedial measures being required – see discussion under financial sector above) at 53 DNFBPs and had conducted risk assessments of 11 institutions. Various enquiries and training sessions were also provided. It is clear to the assessors that these actions did not constitute the kind of supervisory activity defined by the FATF under R.28.

386. It is not clear why the AML Law
regulators in AML/CFT supervision by the PBC. What little information is available suggests that the PBC has done only a very small amount of work in the DNFBP sector such as some visits and a few risk assessments in various areas of China to gain an understanding of ML/TF risks.

Promoting a clear understanding of AML/CFT Obligations and ML/TF Risks

387. The PBC conducts a guidance publishing strategy that is designed to bring to

that guidance improved the ability of FIs to identify risk and raised AML/CFT awareness among senior executives and staff. However, the assessors noted a low to moderate level of understanding of ML/TF risk in the financial sector (see IO.4 discussion). As noted above, the RA Guideline was issued in 2013 but had not been updated by the time of the on-site visit. Further, although there is guidance on CDD measures, it mostly addresses customer identification issues and information linking suspicious activity to predicate offences generating illicit proceeds. This type of guidance may be effective at improving the ability of FIs to satisfy basic obligations and file useful STRs but does not appear to be aimed at more complex or sophisticated improvements needed in internal controls and CDD obligations, especially in larger FIs.

388. Important PBC guidance is issued by PBC Head Office (PBC HO), including that relating to customer identification and suspicious transaction reporting. In addition, Supervisory Opinions are considered guidance and are published as such. PBC guidance strategy is, to a considerable extent, executed by branches (as guidance is normally linked to local issues and risks) after reporting the proposed guidance to PBC HO for review and approval. The authorities have confirmed that this process prevents PBC branches from issuing potentially conflicting guidance.

389. Sector supervisors also issue guidance, mostly on internal controls. Although these are helpful, and address specific internal controls supporting compliance with AML/CFT obligations, they do not address compliance issues under the AML/CFT law; however, the authorities confirmed that the sector supervisors do consult with the PBC before issuing such guidance to ensure that there is no conflict with regulations.

390. Official Replies: The PBC regularly issues what amount to interpretation bulletins to FIs that request assistance in understanding their obligations. More than 80 of these official replies had been issued at the time of the onsite assessment.

391. Risk Warnings: The PBC regularly holds briefings for FIs and sector regulators, issues analysis reports on ML/TF typologies, the types of crimes that are mainly

Key Findings

a) Basic (or legal) ownership information is collected and publicly available on the internet for all types of legal entities, although the information is not always accurate, and it seems relatively easy to circumvent the registration rules (for example through straw persons).

b) BO information of legal entities (domestic or foreign) is not (publicly) available in China. Authorities make use of available basic information, CDD information collected by FIs, and law enforcement powers to obtain such information. Each of these sources poses shortcomings and significant challenges, and the combination of measures at the current stage falls fundamentally short of what an effective system for obtaining accurate, adequate and current BO information in a timely manner would look like. Basic legal ownership or shareholder information may in practice in some cases be the same as the BO information, but the concepts are fundamentally different, and authorities should not rely on basic legal information as an alternative measure to identify the BO. That said, authorities have already initiated plans and measures that may improve effectiveness in the future.

c) There is no granular understanding of the ML/TF risks of each type of legal person, and the risk classification that has been produced for the purposes of the NRA focuses on control measures related to technical compliance. Some of the findings of this risk assessment are also not supported by the risk scoping for this assessment, are inconsistent with other government policies (such as the national anti-corruption drive) and are inconsistent with case examples provided to the assessors (which highlight incomplete basic information and lack of BO information as the main vulnerability).

d) The Trust Law provides for the creation of domestic civil trusts. No measures have been taken to mitigate the misuse of domestic trusts, although the lack of a regulatory framework for civil trusts is an impediment to its use and as such can be considered a mitigating measure in itself. Foreign legal arrangements (i.e., foreign trusts) operate in China, such as the legal or beneficial owner of a Chinese legal company. Authorities have been able to identify foreign trusts that operate in China.

Recommended Actions

a) Short of requiring all BO information to be registered directly with, for example, SAMR (which would be the relatively most straightforward solution), authorities must continue to take other measures to ensure that adequate, accurate and current BO information is obtained in a timely manner. This includes continuing to require FIs to collect and verify BO information, and improve compliance with these requirements. The PBC's proposed BO register for information collected by FIs could also assist in achieving effectiveness in this regard. Authorities should no longer treat basic legal or shareholder information as an alternative to BO information.

b) Authorities need to improve the accuracy of basic information available in the public registers, as collected by SAMR, among other reasons to better prevent against front companies. This should include stricter verification and enforcement of registration requirements. This should also include widening the
when breaches are detected (in addition to the focus on the natural persons involved with the abuse).

c) Authorities need to improve their understanding of the risks of legal persons by undertaking a more granular risk assessment for each type of legal person, rely less on existing control measures, and that takes into account a broader range of existing risks that may impact legal persons.

d) Authorities should take additional measures to prevent the misuse of legal persons, including an increased focus on complex schemes to abuse legal persons and hide BO during financial investigations (without losing the current focus on abuse through front companies).

e) Authorities need to take further measures to abolish, dematerialize, or register bearer shares.

f) Authorities should consider reviewing the current legal basis for the creation of domestic trusts, in view of the uncertainty that it creates.

398. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The recommendations relevant for the assessment of effectiveness under this section are R.24 and 25.

Overview of the Types of Legal Persons and Arrangements

Legal Persons

399. Company law is subject to continuous development since the policy of economic opening-up started in 1978, and the changes are still ongoing. As is set out in Chapter 1, the Civil Law is somewhat open ended in this regard, as it defines for

profit

tax departments. As part of this process, some of the basic information provided during the setting-up process needs to be re-submitted to these authorities. There are some additional steps to be taken for legal persons with foreign ownership.

403. In recent years, the State Administration for Market Regulation (SAMR, formerly the State Administration for Industry and Commerce) has modernized and decentralised its part of the registration process, by providing facilities for on-line registration. Other authorities that can be involved in the registration process include the MPS, the PBC, the tax authority and the social security administration. Authorities stated that there are no regional differences regarding the requirements for any type of legal person or market entity. Authorities indicated that official websites of authorities such as the State Council, SAMR and the MCA have promulgated laws and regulations that specify the detailed procedures for setting-up each type of legal person, and these laws are posted on-line.

Legal Arrangements

404. As outlined above, the law provides for the existence of civil trusts, but there is no further regulatory framework.

Identification, Assessment and Understanding of ML/TF Risks and Vulnerabilities of Legal Entities

405.

legal persons is set out in the NRA and in more detail in an annex to the NRA. The focus of the NRA is on the rules and control measures that are in place for each type of entity, and there is little information on threats and vulnerabilities. Without such information, the risk classification that is included is difficult to understand. This especially concerns the classification of state owned companies as low-risk. This is inconsistent with the many known corruption cases that originate from state owned companies, and with the priority that the government is giving to cracking down on such corruption. The same applies to other types of state-linked entities that are considered low-risk. Authorities explained the classification of state-owned companies as low risk due to the fact that these are initially not set-up with an aim to be abused for crime, which is a possibility for other types of legal persons. Assessors note that this does not take into account that existing state-owned companies are being misused for crime and money laundering, which is a major risk.

406. However, competent authorities and private sector representatives that the assessment team met with had a consistent view of the main vulnerability that China faces, which is the misuse of legal entities through setting up front companies (in the NRA also referred to as shell companies) to commit fraud and other crimes. The authorities also identified the unavailability of BO information and lack of complete basic information as important vulnerabilities. Authorities note that BO is a very recent concept in China, and that only FIs are required to collect such information. The NRA also notes that most banks do not carry out checks of ownership, in the absence of regulatory requirements.

407. Authorities provided a large number of case examples of misuse of legal persons. Some cases were more complicated, including with foreign ownership structures. The majority of cases concern rather straightforward use of front companies, set up or acquired specifically to commit crimes. More often than not, these cases seem to involve a registered contact person who appears to be a straw person, which is in line with the observation that basic information is not always available or accurate (see below on enforcement). The detection of such cases happens as part of law enforcement action at the investigative stage. Regional law enforcement authorities that met with the assessment team explained that they are able to locate the beneficiary of these front companies through following the money trail from the company, which from examples provided seemed to be the immediate recipient of the funds. This type of abuse does not seem to require more complicated structures with beneficial owners that are further removed from the abused company.

408. Law enforcement did not appreciate the need for having access to BO information, even for chains of BO with offshore links. It may be that law enforcement does not search for such cases or does not further investigate financial trails beyond the beneficiary. However, considering that registered basic information is not necessarily accurate or complete and that BO information is only available through FIs (if at all), criminals and terrorists in China may not need to make as much use of complicated structures to hide and channel their illicit assets.[56]

56 See also on IO.11 for front companies in relation to the financing of proliferation.

also provided case examples where financial services were not provided due to a lack of BO information (for various reasons).[57]

Legal Arrangements

412. No specific mitigating measures have been taken in relation to civil trusts although the lack of specific regulations may be a mitigating measure in itself as it discourages the use of civil trusts. For foreign legal arrangements operating in China, there are no specific mitigation measures beyond CDD rules in AML/CFT that require the identification of a trust.

Timely Access to Adequate, Accurate and Current Basic and Beneficial Ownership Information on Legal Persons

413. China aims to use a combination of mechanisms to gain access to basic and BO information. However, there are important shortcomings with each mechanism.

414. The first mechanism is to use basic registered information to find the legal owner or shareholder of a legal entity. This mechanism is only useful to identify the BO in cases where the legal owner or shareholder and the BO are the same, but the registered information itself will not indicate if the registered legal owner or shareholders are indeed the BO. That said, basic registered information can be a starting point to identify BO information, and accessing this information poses no problems whatsoever. Information is publicly available through the National Enterprise Credit Information Publicity System (NECIPS), and through commercial parties. However, the registered basic information is limited to the information that is required to be collected by SAMR and the accuracy depends on verification at the registration stage, and when information is changing. Authorities provided good examples of the use of the system, but a review of the publicly accessible registers by the assessment team also indicated the information can be limited to the name of the company and the name and address of the contact person for the legal person. The number of breaches and the relative ease to set up front companies also provide an indication that the effective implementation of this system requires improvements.

415. The second mechanism that authorities use is BO information available elsewhere, including through CDD measures. As noted above, while a potentially good

[57] See also on IO.11 for front companies in relation to the financing of proliferation.

mitigation measure, the implementation of these CDD measures is too recent to be considered effective at this stage (as noted as well in the NRA). The third mechanism is through the use of law enforcement powers, either to gain access to the information held by the legal person (but note that legal persons are not required to hold such BO information) and/or their representative (who is also not required to hold such BO information). As has been elaborated in other assessment reports, the use of law enforcement powers poses unique challenges to effective implementation that can be a fundamental barrier to achieve effective compliance. Not limited to the fact that law enforcement will have to find the BO information not knowing beforehand if it exists and where it is available. This also negatively impacts the timeliness of access to the BO information.

Timely Access to Adequate, Accurate and Current Basic and Beneficial Ownership Information on Legal Arrangements

416. No adequate, accurate, and current basic and BO information has been shown to exist for legal arrangements (civil trusts), mitigated by the potentially limited existence of such domestic civil trust. For foreign legal arrangements operating in China, there are no specific sources of information beyond BO information collected by FIs, which poses the same issues as for BO s been n b

registrations. In comparison, of the nine million listed legal entities, about seven million were listed for not submitting annual reports, and more than one million because the legal person could not be contacted through the listed contact person, not even by the authorities. As far as risks of abuse of legal entities is concerned, one would expect that the lack of filing of an annual report and the lack of a contact person would be major red flags for the authorities to further pursue – especially in light of front companies as a major vulnerability. However, authorities have not demonstrated that they indeed follow-up on such cases. Also, a listing for breach of requirements does not necessarily lead to a sanction of the legal person.

418. Since 2015, 40 competent authorities coordinate at the policy level to address misuse of legal entities, each with a focus on compliance in their respective area. As a result, legal persons that have breached too many requirements by too many competent authorities can be listed as dishonest legal entities. To date, 9538 legal persons have been listed as such, but not for breaching BO information.

419. Overall, it appears that the rate of detection of misuse of legal persons is low. Authorities have indicated their priority is to pursue criminal charges against the natural persons in charge of legal entities. This can be explained by some of the provisions in the Criminal Law, which include sanctions for management and staff of legal entities for the wrongdoing of these legal entities. The sanctions for natural persons are also higher than the comparatively low monetary sanctions available to sanction legal persons.

Legal Arrangements

420. No information is available on sanctions regarding domestic civil trusts, a deficiency that is mitigated by the potentially limited existence of such domestic civil trusts. Likewise for foreign legal arrangements operating in China.

Overall Conclusions on IO.5

421.

摘 要

Key Findings

a) China has a largely compliant legal framework for international co

d) China should align its MLA requests with geographic ML/TF risks.

e) China should ensure that it can provide adequate and timely BO information.

422. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The recommendations relevant for the assessment of effectiveness under this section are R.36-40.

[illegible]

423. As recognised by the authorities in the NRA, illicit proceeds are often transferred overseas, for example through the use of bank cards, underground banks, cross-border transportation of cash, and splitting of foreign exchange purchases (see also Chapter 1 and IO.1). The international context increases the importance of international co-operation as a risk mitigation measure. The coverage of these risks in the NRA and the results of the interviews with authorities during the on-site indicate that authorities understand these risks.

Providing Constructive and Timely MLA and Extradition

424. China has a legal and procedural framework for international co-operation and assistance, but it has complicated procedures. The MOJ is the leading central authority for accepting, reviewing and transferring MLA requests. China has provided MLA in a timely manner in some cases, but due to often complicated decision-making structures regarding the provision of the MLA, providing assistance in practice often takes a long time. Feedback on international co-operation with China received from the global network was varied. There was some positive feedback and good examples of co-operation, but a number of countries expressed concern with respect to and delays and lack of responses by China for which no valid explanations were provided

425. China does not have one central authority dealing with MLA requests. This is due, in part to the absence of a MLA law and the decentralised nature of the system. While the MOJ is the leading agency, MPS and GPP are also central authorities under certain treaties and UN conventions. China categorizes MLA into two groups based on whether there has been a treaty on criminal legal assistance or not. In China, there are authorities receiving requests but sending them for execution to other authorities, as well as authorities receiving and executing requests, and the execution can be at the central level or done by local branches.

426. China has established a multi-channel method of carrying out international co-operation:

- the MOJ is one of the authorities for the MLA requests under the Palermo Convention and when it is mentioned as such in agreements and treaties signed by China;
- the MPS is the other authority under the Palermo Convention and in a number of bilateral treaties and agreements;
- the MFA is the channel for the Vienna Convention, and extradition requests and MLA in the absence of an agreement; and
- the

430. Similar statistics were presented for other ministries involved in MLA. In general, the figures for MLA received show that more than half of all requests are received by China through the MOJ.

431. China, considering that different ministries (including local authorities) can execute MLA requests from abroad, developed general and agency-specific provisions, notices, and guidance on how to handle judicial legal assistance. It is a positive measure because many requests are executed at the provincial level, and those branches have a need for additional guidance when they receive those requests from the central offices for execution.

432. China provides a range of assistance to MLA requests relating to the provision of documents, witness statements and asset recovery, including the identification, tracing and freezing of proceeds from foreign predicate offences. The legal provision requires China to initiate pro forma domestic investigations or procedures and obtain a Chinese court decision to enable the full range of freezing and confiscation powers available domestically. Challenges in relation to the confiscation of assets were noted by a few countries in the global network responding to the survey on international co-operation.

433. The table below shows the type of action foreign countries request from China (through the MFA), 19 of them (around 5%) involved ML, and one was related to TF offences.

2							

434. And the procedure for extradition is different from the procedure for MLA requests. After the MFA receives the request, the SPC examines whether the request is in conformity with the provisions of the Extradition Lawand extradition treaties. In practice,
Court.

437. The following example demonstrates how the extradition system works in practice in China. The process is too lengthy and can take several years. Although it should be noted that on several occasions the extradition process was completed within one year.

> In June 2014, Japan requested China to extradite and detain Y, a Brazilian criminal suspect. Japan subsequently submitted a formal extradition request in July 2014. The MFA, after examination, requested supplementary materials. After Japan provided the materials, the Supreme People's Court reviewed the case and decided that the case met the conditions for extradition as stipulated under the Extradition Law. Japan accused Y of forgery and use of printed personal documents for defrauding. In May 2016, the State Council decided to grant extradition. The MFA notified Japan on June 2, 2016.
>
> In June 2016, Japan submitted new evidence, requesting China to agree to additional crimes that Japan charged Y with, after the extradition was decided (robbery and homicide). The Supreme Court reported its decision to the State Council, and China agreed to this request and notified Japan of the decision on January 9, 2017. On January 25, 2017, China extradited Y to Japan. This case is useful to understand the lengthy extradition procedure, even if the case does not involve ML/TF.

Seeking Timely Legal Assistance to Pursue Domestic, ML, associated predicates and TF Cases with Transnational Elements

438. China does not make frequent use of the official MLA mechanisms apart from extradition issues. But it uses other possibilities to achieve the needed results, which was demonstrated to the assessment team. These cases are different from extradition cases. T

conduct with other countries (see the box below). No ML cases were involved in these operations.

> To further combat corruption and economic crimes, China has launched various special operations. For example, the Central Commission for
>
> carried out special operations related to international fugitive repatriation and asset recovery on corruption-related crimes, and the MPS launched

2016, 2566 individuals who had previously fled China were recaptured from 90 countries and total asset of RMB 8.6 billion (approx. USD 1.3 billion) were recovered. In 2015, Interpol China National Central Bureau released a 100 fugitives list (Red Notice) of persons involved in corruption cases. By the end of 2016, 43 out of 100 individuals were caught.

439. The statistics on seeking MLA had been presented only by the MOJ. From the figures for MLA requests related to ML it is clear that China mainly pursues predicate offences and considers ML as a continuation of the predicate offence so ideally China should use the MLA for ML more often.

440. When there are no treaties or agreements between China and another country, the MLA requests are sent through the MFA via diplomatic channels. From 2012 to 2016, China sent about 20 MLA requests through diplomatic channels. The overall number of MLA requests is low in comparison with the crime statistics.

441. China makes extradition requests in accordance with the Extradition Law and bilateral extradition treaties. To request an extradition, the relevant local departments submit a written statement with relevant documents and materials as well as certified translations through its own central body (i.e. the SPC, the SPP, the MPS, the MNS, or the MOJ). After approval of the request, the MFA initiates the extradition request to a foreign country. China provided overall figures for requesting extradition. In total 103 requests were sent to 34 countries since 2012. These requests refer to predicate offences. The below table shows that the crimes China requests extradition for, do not match its risk areas, and only 2% of the requests are related to ML.

	1
	1
	1
	1

442. China actively pursues fugitive criminals by trying to obtain extradition from other countries. It does not stop at sending extradition requests but organises visits to the relevant countries, uses INTERPOL channels, joint operations and other means.

443. Overall, analysis of the information and data presented by the country shows that China is seeking MLA/extradition related to transnational ML/TF cases to a lesser extent than wo The majority of co-operation it seeks is related to predicate offences.

Seeking and Providing Other Forms of International Co-operation for AML/CFT Purposes

444. The Chinese authorities regularly seek other forms of international co-operation to exchange financial intelligence, law enforcement, supervisory, and other information with foreign counterparts, including for AML/CFT purposes. This exchange of information operates at an operational level and has led to some tangible results.

The Financial Intelligence Unit (CAMLMAC, AMLB, PBC Branches)

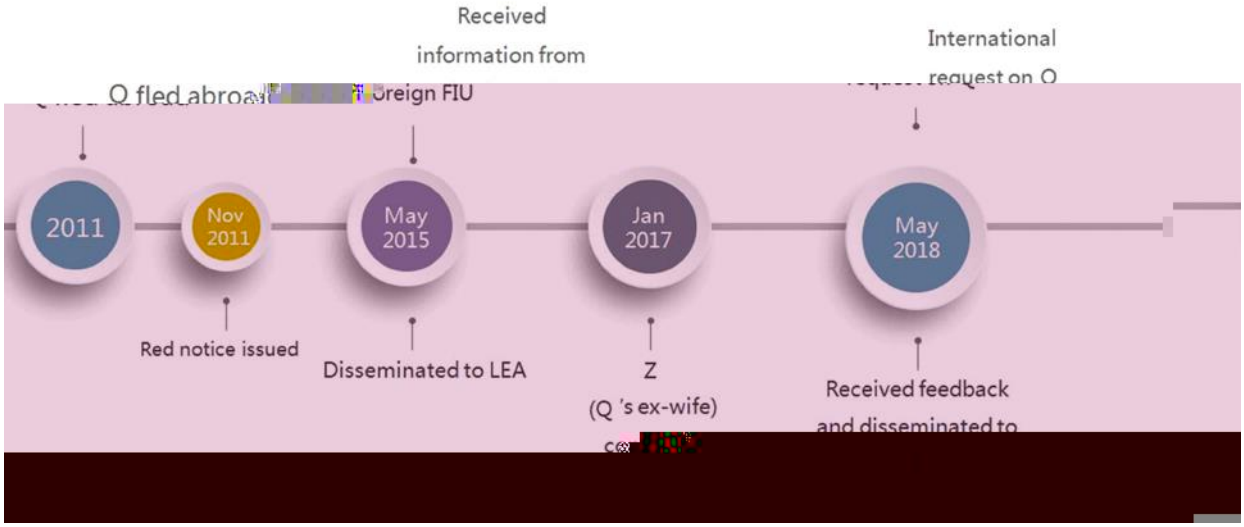
445. CAMLMAC is responsible for receiving, analysing, and transferring financial intelligence, signing bilateral memorandums of understanding (MOUs) on AML/CFT intelligence exchanges and co-operation or similar documents (agreements) with counterparts of other countries. CAMLMAC exchanges information with foreign counterparts, even though it is not an Egmont Group member. It has signed 52 MOUs with foreign FIUs. That deficiency is partially addressed by signing the MOUs with FIUs with which the exchange of information is primarily needed. This exchange of information is mostly based on the requests from abroad and to a much lesser extent on the requests from China to other FIUs (due to a small number of ML/TF investigations). The below tables clearly show that difference. The Chinese

446. As figures in the tables show, the number of requests is very low in the light of the size of the country and its economy, and more importantly, the number of STRs received and the volume of financial analysis. Moreover, comparison with the number of requests for financial information from other FIUs shows that China sends approximately one request to 30 or 40 requests received. That demonstrates that the channel of obtaining financial information from other FIUs is practically not used, even though transnational financial flows are very large in volume and the risk of laundering proceeds from domestic predicate crimes abroad is high. It appears that the FIU is not using actively the possibilities provided by 52 MOUs signed by China. International co-operation feedback from other jurisdictions indicated mixed experiences. Whereas the SARs and some FIUs from Asia-Pacific countries indicated satisfaction regarding the quality of co-operation with China, some other FIUs indicated that co-operation was formalistic and that responses were not always given and, in some cases, where they were given, they lacked substance.

447. Two-thirds of the outgoing requests are to SARs of China, Hong Kong, China and Macau, China. This is not consistent with the geography of cases investigated and pursued by LEAs, including those involving predicate offences with large criminal proceeds.

> Q, former director of a branch of a city office, was placed on file by the Anti-Corruption Department of the Procuratorate on suspicion of embezzlement and misappropriation of public funds. He fled abroad in 2011. He was placed on the Red Notice by Interpol in November 2011.

In May 2015, Singapore FIU shared intelligence with the CAMLAC which stated that Q held multiple bank accounts, investment accounts, home loan accounts and credit card accounts at a Bank of Singapore and was a BO of a company and a fund in the British Virgin Islands. Based on the information shared by Singapore, CAMLMAC analysed over 70 accounts and over 270 000 large-value and suspicious transaction records, and identified the Q funds were closely related to the accounts of Y and W who were suspected of operating underground banks. The fund-flow transaction chart indicated characteristics of operating underground banks. The CAMLMAC disseminated the analysis results and spontaneous dissemination information from the foreign FIU to the LEAs.



The LEAs discovered that Q had applied for and obtained a house mortgage with a bank abroad. In May 2018, LEAs filed an international investigation with foreign FIU through the CAMLMAC, and obtained information on the address, owners and pledge of the houses Q purchased using the house mortgage.

Since Q and his ex-wife Z were under investigation of the U.S. LEAs, the Chinese LEAs provided intelligence and evidence to support the U.S. investigation. U.S. prosecutors filed formal charges against Q and his ex-wife, Z, for and immigration fraud. The prosecutors

the properties to be seized were purchased with money embezzled by Q. Z will face imprisonment up to five years.

Law Enforcement Authorities

448. LEAs seek informal international cooperation in a wide range of cases, as a rule related to predicate offences, and most of all in corruption cases. In addition to the usual MLA channels, LEAs use INTERPOL, liaison officers, and joint operations as avenues for international cooperation, especially when seeking the return of funds or fugitive criminals to the country. However, the instances when these mechanisms have been used in relation to ML/TF are quite limited. Any execution of foreign requests at the level of provinces happens in accordance with instructions from the central authorities when they send a request to a provincial branch.

449. The exchange of information through Interpol is many times more intensive than MLA. On average, between 2012 and 2017, 9% of those requests have involved money laundering. At the same time, the number of requests sent by China is around 15% of those received from foreign countries through Interpol, which also signals that China does not make sufficient use of informal co-operation channels.

450. The MPS established close cooperation relationships with 113 countries, established 129 bilateral and multilateral cooperation mechanisms, 96 liaison hotlines, sent 72 police liaison officers to 35 countries and signed nearly 400 co-operation documents with the police departments of more than 70 countries. The MPS generally collects information directly through these channels and police liaison officers, which seems to be efficient and quick.

451. Police representatives demonstrated that the requests they are sending abroad are in line with the risks defined in the NRA; however, it does not fully match the risks as viewed by the assessment team (see Chapter 1). Authorities were also unable to demonstrate a focus on ML or TF.

452. Most of the Chinese police requests relate to predicate offences, the MPS does not focus on ML or TF in international cooperation. The MSS is dealing with terrorism issues but authorities were unable to provide any information on TF to prove effectiveness, citing confidentiality of data.

Customs, Tax and Supervisory Authorities

453. Customs, Tax and Supervisory authorities actively engage in international co-operation. For example, in 2017, China Customs carried out more than 1,000 intelligence exchanges with foreign countries, handled 329 requests of investigation assistance, and carried out international (regional) law enforcement co-operation in 99 cases on behalf of the Anti-Smuggling Bureau of the General Administration of Customs. The CBRC carries out regular consultations with foreign regulatory authorities. Exchange of information has taken place on establishment of banks and reviewing the qualifications of senior executives. From 2012-2016, the CSRC sent out 51 requests for foreign regulatory information. However, these authorities did not engage with ML or TF-related cases or exchange of information with foreign counterparts for those purposes.

Providing Other Forms of International Co-operation for AML/CFT Purposes

Financial Intelligence Unit (CAMLMAC, AMLB, PBC Branches)

454. For financial intelligence requests received from overseas, CAMLMAC will assess the urgency of the request. Consideration is given to whether the request may

455. The two tables above demonstrate that the number of responses is significantly lower than the number of requests received by China. That is an issue of concern for the effectiveness of the international exchange of information, although the Chinese authorities explain that much of the needed information can be obtained inside the country, which diminishes the need for requesting other countries. That explanation needs to be reviewed by the authorities. Moreover, the feedback from some countries on their experience in the exchange of information mentions that Chinese FIU only provides information already available in its database (which limits the quantity and quality of the data provided).

Law Enforcement Agencies

456. The below table shows the overall situation with the MPS assisting foreign police investigations in recent years. Of these, the United States, Canada, and Australia submit average 230, 100, and 80 investigation requests respectively per year.

457. In general, the police in China co-operate through different channels, not only through answering to requests, but they pay much attention to operational contacts and joint events and investigations. However, the figures shown above relate to all cases of co-operation, not just ML or TF, which China has not provided.

Customs, Tax and Supervisory Authorities

458. In 2017, the Anti-Smuggling Bureau of the General Administration of Customs processed 225 requests including administrative mutual assistance, case investigation and criminal legal assistance, for overseas law enforcement authorities, completed 40 criminal compulsory measures reports. There were 434 occasions from 2012 to 2016, in which regulatory information was provided to foreign countries. Regarding the follow-up measures of requests, only one request was rejected in 2016, and the acceptance rate was 99.8%. However, none of the cooperation concerned AML/CFT.

International Exchange of Basic and Beneficial Ownership Information of Legal Persons and Arrangements

459. BO information is not easily and quickly available, except in cases when law enforcement happens to be able to detect the beneficial owner using coercive powers, or shareholder information of publicly traded compder rrm

This annex provides a detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological ordeve04c4 (pl)1ET Q 3.996 withlynt

working group formed in 2016 under the leadership of the PBC which included representatives from each agency member of the AMLJMC; SRBs, including the Internet Finance Association of China, the All China Lawyers Association, the Chinese Institute of Certified Public Accountants (CICPA), and the China Notary Association, as well as AML-regulated institutions from the banking, securities, and insurance sectors as well as non-banking payment institutions.

Criterion 1.3 In August 2017, the General Office of the State Council issued the Opinion on Strengthening the Supervisory Framework and Mechanism for Anti-Money Laundering, Countering the Financing of Terrorism and Anti-Tax Evasion (State Council GAD Letter No. [2017] 84)

analysis system shall be optimized constantly, and the risk prevention system shall be improved, aiming at controlling the risk of money laundering, terrorist financing

an annual AML/CFT National Threat Assessment.

Criterion 1.4 Electronic copies of the NRA were sent to government departments and the major financial institutions. Smaller FIs and other regulated entities are provided copies through their local PBC branches. The NRA was also distributed to industry association bodies where it is available to DNFBPs. This distribution method has also been used to distribute the Annual National Threat Assessments with a summary version posted on the PBC website.

Weighting and Conclusion

Criterion 1.5

measures can be taken, except for customers matching a number of high-risk scenarios.

Criterion 1.9 Since 2015, the PBC requires financial institutions to conduct ML/TF risk assessments and classify customers based on risk levels. The PBC conducts inspections of financial institutions to ensure implementation of their risk assessment

designated non-financial businesses and professions shall be formulated by the administrative department of anti-money la 8 and 35 of the AML Law of – Š ‡ ‡ ‘ ’ Ž ‡ ï • ‡ ’ — „ Ž ‹ … ‘ ^ Š ‹ • ƒ ” 56)). ‘ ^ – Š ‡ ” ‡ • ‹ The authorities issued a notice in July 2018 to give eff t to this designation, but the assessment team does not consider that the notice meets the requirements set out on Art. 35 of the AML Law (see discussion under R.22). There is currently no effective oversight or monitoring has occurred to ensure that DNFBPs are implementing their obligations under R1.

Criterion 1.10 According to the Guidelines for the Assessment of Money Laundering and Terrorism Financing Risks and Categorized Management of Clients of Financial Institutions
status of customers and their locations, businesses, industries (occupations) and

effectiveness of their risk prevention and control mechanisms, so as to identify areas with vulnerabilities and weaknesses and take targeted risk mitigation measures.

FIs are also required to improve the procedures of the risk assessment, designate suitable departments and personnel to be responsible for the establishment and monitoring of the risk assessment procedures, and organise relevant departments to participate in the risk assessment.

As mentioned under c.1.7 above, FIs are required to allocate their AML resources based on the risk assessment results and to exercise enhanced measures on areas with high ML/TF risk.

Trust companies are considered FIs in China; therefore, they are subject to the same obligations above.

DNFBPs have not been designated under the AML Law and therefore are not subject to similar AML/CFT obligations.

Criterion 1.12 As mentioned under c.1.8 above, if FIs identify some businesses as low risk, consistent with the NRA, simplified measures can be taken. Simplified measures are not permitted whenever there is a suspicion of ML/TF, and the FIs are required to take enhanced measures, including re-identification of customers and suspicious transaction reporting.

Weighting and Conclusion

While China only completed its first NRA in June 2018, it has been conducting threat, vulnerability, and risk assessments since 2012 on a variety of topics specific to AML/CFT. There are however gaps arising from the fact that DNFBPs have not been designated under the AML Law and are therefore are not subject to AML/CFT supervision including supervisory risk assessments. Financial institutions are permitted, with PBC approval, to adopt simplified customer due diligence and other risk control measures for low-risk customers. No effective oversight or monitoring has occurred to ensure that DNFBPs are implementing their obligations under Recommendation 1.

[illegible]

In the Third Round, China was rated largely compliant on National Coordination (formerly R.31). The primary shortcoming identified was with respect to the level of operational cooperation between law enforcement and prosecutorial authorities. It was felt that the level of cooperation needed improvement.

Criterion 2.1 In 2002 China established the AMLJMC which is responsible for assessing the national ML/TF risk, developing national AML strategies, guiding principles, and policies.

The AMLJMC is responsible for conducting the ML/TF NRA on a regular basis. This includes the formulation and regular update of AML/CFT strategies and policies based on the risks identified in the risk assessment. The AMLJMC is also responsible for identifying priorities, delegating tasks to appropriate entities, and monitoring progress on national initiatives. Since the NRA has only been recently concluded, it is

not possible to determine the extent to which national policies are informed by identified risks of this latest exercise.

Criterion 2.2
authority. This responsibility falls to the AMLB which is a unit within the PBC. It is responsible for organis luding the establishment and refinement of AML/CFT policies.

Criterion 2.3 The AMLJMC currently has 23 members (including the PBC), financial regulatory authorities, LEAs, judiciary and foreign affairs departments, and other industry competent authorities. Together, they are responsible for assessing the national ML/TF risk, developing national AML strategies, guiding principles and policies. The work of the AMLJMC is regulated by the Mechanism of Anti-Money Laundering Joint-Ministerial Conference (2007 Amendment).

The AMLJMC has established a number of working groups, including policymaking, regulation, law enforcement, international, and data groups, which strengthen the

operational levels.

The AMLJMC enables AML competent authorities such as PBC, LEAs, regulatory authorities, and other relevant authorities to cooperate, and where appropriate, coordinate domestically concerning the development and implementation of AML/CFT policies and activities.

Criterion 2.4 -proliferation Export Control

proliferation work, and coordinating 19 members, including the PBC, the MFA, the Ministry of Commerce, and the National Development and Reform Commission, to combat PF.

national non-proliferation law.

Weighting and Conclusion

[illegible]

In its Third Round MER, China was rated partially compliant for Rs.1 and 2 (ML offence). The main shortcomings were a lack of effectiveness, lack of self-laundering, partial lack of criminal liability for legal persons, and other technical shortcomings with the Vienna and Palermo Conventions.

Criterion 3.1 The required elements from the Palermo and Vienna Conventions have partly been covered in the Criminal Law. Missing are the following elements, for both Conventions: (i) Art. 191 Criminal Law (CL

in Notice 2009:15, Art. 1(2); but (ii) Arts. 191 and 312 CL
All

Criterion 3.2 China follows the all-crimes approach (Art. 312 CL), however provinces and autonomous regions can also place a value range to determine if the behaviour is criminal or otherwise. This means laundering of funds under RMB 3 000 (approx. USD 489) is not criminalized, but this could extend to a value of RMB 10 000 (approx. USD 1 467) subject to the discretions of a province.

Subject to the threshold, Art. 312 covers all 21 categories of predicate offences. However, some of these predicate offences are too narrow.[61] Art. 191 CL covers seven predicate offences (drugs, organised crime, terrorism, smuggling, corruption and bribery, financial management disruption, and financial fraud), while Art. 349 CL covers only drug-related offences. Art. 312 CL is also the predicate offence of receiving stolen goods.

Criterion 3.3 This criterion is not applicable, China follows an all-crime approach in Art. 312 PC.

Criterion 3.4 Art. 191 CL offences and the

proceeds. There is no provision in law ; however, these terms are defined in SPC guidance. There does not seem to be a threshold for the value.

Criterion 3.5 There is no evidential requirement that a conviction for the predicate offence is needed to prove that the property is the proceeds of crime. The burden of proof of the predicate offence depends on what basis the prosecution is initiated: the all-crimes coverage of Art. 312 CL does not require the proof of a precise and identified predicate criminality, whereas Art. 191 CL (which follows a list approach) requires establishing the link to one of the types of listed offences (without requiring proof that the proceeds are connected to a specific predicate offence). This has also been confirmed by SPC interpretations.

Criterion 3.6 The Criminal Law covers all conduct by Chinese citizens inside and outside the territory, covers offences against China committed by foreigners abroad, and includes conduct specified in international treaties (Arts. 7-9 PC). While this does not completely cover all possible situations, there is also no limitation in Chinese law that would limit the reach of the CL in this regard. This is confirmed in jurisprudence (Quanzhou Cia Jianli case).

Criterion 3.7 Self-laundering is not criminalized in China. ML is understood to be a non-punishable subsequent action of the predicate offence, and the sanction for the laundering of proceeds of predicates would be absorbed by the sentence for the predicate offence (which requires a predicate in China. Foreign predicates that are not criminalized in China are not covered). This is not a fundamental principle of law,

61 Participation in organized criminal group and racketeering: Arts. 26 and 294 CL define organized group, but racketeering is not explicitly covered. Trafficking in human beings and migrant smuggling: Arts. 240 242 CL only covers trafficking of women and children (not men), and migrant smuggling is not covered. Illegal border crossings are criminalized, but only target the victim of human beings and migrant smuggling. Piracy: Art. 123 CL only covers hijacking of a ship (or car), but no other acts of robbery and criminal violence are covered

authorised by a person in charge of the Public Security Agency at or above county level or city level if the case is consider large and complex. Having been approved, written seizure decision is prepared,[65] and an authorisation is provided to an investigator. Appropriate ministries are advised, such as the MOHURD, and they are required to provide necessary assistance to bring the authorisation into effect. The authorisation remains in place for two years, but can be subject to renewal for 12 month periods, if required.[66] With non-

freeze W* n BT /TT0 11.0. 0 595.32 8425.32 842.04 r11.04 T003>]TJ4 (ont)3.007 (h)-31.005 (p)12.99

400960003>-16 >3.995 (<96 <005 <0083009>-085>-3.992 99174 <0095>08B83>-29.0091B>6.005 <0075>5.996 <009700

individual terrorist, this requires a direct link to the Counter Terrorism Law. Art. 120A itself seems to cover only direct assistance and not the wilful collection of funds.

Criterion 5.2 bis Art. 120A of the CL covers the financing of the travel of individuals who travel to a state other than their states of residence or nationality for the purpose of the perpetration, planning, preparation of, or participation in terrorist acts or the providing or receiving of terrorist training.

Criterion 5.3 Chinese law is silent on the source of TF (legitimate or illegitimate), licit or illicit

Criterion 5.4 Art. 120A CL does not seem to require that the funds or other assets were actually used to carry out or attempt a terrorist act or are linked to a terrorist act.

Criterion 5.5 Although there is no specific provision in the law stating that the intent and knowledge required to prove the offence can be inferred from objective factual circumstance, the concept was codified in jurisprudence by the Supreme Court (2014/34, Section 3, Art. 2). The same interpretation was stated in Opinions of SPC, SPP, MPS, and the Ministry of Justice on Certain Issues concerning the Application of Law in Dealing with Criminal Cases Involving Terrorism and Extremism [2018].

Criterion 5.6 The penalty for TF is a fixed-term imprisonment of not more than five years, open-ended criminal detention (one to six months detention), or open-ended public surveillance (three months to two years detention), or open-ended deprivation of political rights (one to five years detention, or life imprisonment, or capital punishment), in addition to a fine (determined by the circumstances without a prescribed maximum, as per Art. 52 CL). If (something which is not further specified), the penalty is raised to a fixed-term imprisonment of not less than five years, in addition to a fine, also determined by circumstances without prescribed maximum [or forfeiture of property]. This is sufficiently dissuasive and proportionate (Art. 120A, CL).

Criterion 5.7 Legal persons are criminally liable for TF and can be convicted and fined. The fines are not determined by law, but by circumstances by judges without a prescribed maximum. However, a minimum amount of no less than RMB 1 000 (approx. USD 146) is set (Art. 52 CL). It is not clear if these are dissuasive and proportionate.

Criterion 5.8 Ancillary offences to all offences, including TF, are specified in the general section of the CL. The CL criminalizes preparation (Art. 22); attempt (Art. 23); discontinuation (Art. 24); joint offenders (Art. 25); principle crime leader, ring leader, and criminal organisation (Art. 26); accomplice (Art. 27); coercion (Art. 28); and instigation (Art. by Arts. 25, 27, and 295 CL (giving instructions how to commit a crime).

Such regulation applies to TF and all terrorist offences as stated in Arts. 120 A to 120 F (120-1 to 120-6) of the Criminal Law, where provisions on some special forms of terrorist activities are established.

Criterion 6.2 In relation to designations under UNSCRs 1373:

c.6.2.a and c.6.2.b For receiving requests from other countries, the MFA is the designated authority in line with regular MLA provisions (see R.37). For domestic designations the same procedures and issues apply as for criterion 6.1.b. Designation criteria do not match the detail of INR6 paragraphs 13(c); however, the lack of a link to the UNSC does not affect this criterion (Counter Terrorism Law, Arts. 3, 12, 13, and 16)

c.6.2c No practical example or other (legal) information is available regarding the promptness of the consideration of the foreign request or of the domestic proposal

c.6.2d. Beyond what is covered under c.6.2.b, there are no legal provisions on the evidentiary standard required for designations upon foreign request or domestic proposal.

c.6.2e. There is no requirement in law to provide as much identifying information when submitting requests to other countries. Authorities indicate that in practice this is the policy that is followed, but no example was provided.

Criterion 6.3 Legal authority and procedures:

c.6.3a. The Counter Terrorism Law (Arts. 43 and 47) gives powers the National Leading Group for Combating Terrorism as the entity with nationwide competence for the coordination of terrorist intelligence and all legal authorities. However, there are no specific criteria for designation established under the relevant UNSCRs.

c.6.3b. There are no legal provisions or mechanisms that ensure that authorities operate ex parte against entities designated by the UNSCR or against entities to be proposed to the UN, or against entities designated upon a foreign request or a domestic proposal.

Criterion 6.4 (UNSCR 1267 only) There are no specific legal requirements regarding the legal basis for designation and freezing without delay (except: see c.6.5), nor have authorities been able to establish that this is done in practice.

Criterion 6.5

c.6.5a. There is no requirement for all natural and legal persons within the country to freeze without delay and without prior notice, the funds or other assets of designated persons (i.e., a prohibition). For FIs and designated DNFBPs, the Counter Terrorism Law requires freezing in domestic designations (Art. 14) and the PBC has issued Notice 2017/187 which requires the immediate (same day) freezing of assets of designated terrorists after instruction by PBC, but authorities did not establish that such legal orders are issued each time after the issuing of a UNSCR or of an amendment to the list of designated entities.

c.6.5b. There is no legal requirement to freeze assets that extends to all assets of a designated person or entity. For FIs and designated DNFBPs there is the Administrative Measures for the Freezing of Assets Relating to Terrorist Activities, which comprehensively defines assets (Administrative Measures for the Freezing of Assets Relating to Terrorist Activities, Order of the PBC, the Ministry of Public Security, and the Ministry of State Security No. [2014] 1, Arts. 5 and 11.)

c.6.5c.
required by R.6.

c.6.5d. Not all UNSCRs and UNSC designations are communicated to the financial sector and DNFBPs immediately upon taking such actions. However, the PBC maintains a website with links to UNSCRs (and FATF warnings) and circulates UNSCRs, but this is not systematically done and does not cover every UNSCR and amendment to the list. CDD requirements (see R.10) require banks to use software that include sanctions lists.

c.6.5e. The Counter Terrorism Law (Art. 14) and PBC Notice 2017/187 (Arts. 1 and 2) require reporting of freezing actions by reporting entities to the PBC, but there is a scope issue regarding DNFBPs.

c.6.5f. Persons that receive assets from designated entities in good faith acquire property rights, as provided for by the Property Law (Arts. 4 and 106). It is not clear if such transfers of property titles require UN authorisation, as required by the UN (see c.6.7). There are no other provisions to protect bona fide third parties (such as of parties to existing contracts with designated entities)

Criterion 6.6

c.6.6a. d. (6.6.a; 6.6.b; 6.6.c; 6.6.d) Art. 15 of the Counter Terrorism Law provides the basis and procedure for appeal against a designation as terrorist under the Counter Terrorism Law. The article indicates that a decision on the designation will be taken upon appeal, and that such decision is final and will lead to unfreezing of assets if the designation is revoked. This is compliant with UNSCR 1373 (c.6.6.b and 6.6.b), but not with UNSCR 1267/1989 and UNSCR 1988 (c.6.6.a and 6.6.d). Notice 2017/187 in Art. 5 provides that reporting entities should inform designated entities of the possibility to appeal designation.

c.6.6e. The MFA is said to have issued a notice on the implementation of the UNSCRs 2082 and 2083 which is said to state that if an individual or entity requests to be de-listed, the MFA shall inform the relevant individual or entity to submit a request to the United Nations Office of the Ombudsperson. However, these Notices were not provided.

c.6.6f. Publicly known procedures to handle so called false positives are in place, but only apply to those sectors that are designated under the AML Law (Administrative Measures for the Freezing of Assets Relating to Terrorist Activities, Order of the PBC, the Ministry of Public Security, and the Ministry of State Security, 2014, Art. 10-15 and PBC Notice 2017/187, Arts. 3 and 4).

c.6.6g. De-listing and unfreezing communications suffer from the same deficiencies as designation/freezing communications (see c.6.5.d), and there is no guidance on how to handle such events.

Criterion 6.7 The Administrative Measures for the Freezing of Assets Relating to Terrorist Activities (Art. 12) and PBC Notice 2017/187 (Art. 5) provide a legal basis and procedure to request and grant access to frozen funds. This is sufficient for compliance with UNSCR 1373. However, the legal references are insufficiently specific for compliance with the specific requirements in UNSCRs 1267/1989 and 1988. UNSCR 1452. No information is available regarding the requirement to notify the UNSC of any intended exemption.

Weighting and Conclusion

There are no legal provisions that prohibit legal persons and entities from making funds available to designated entities (i.e., a prohibition). The freezing requirements in the Counter Terrorism Law and in Notice 187/2017 are incomplete in scope and only apply to FIs and designated DNFBPs, and the legal provisions do not allow for freezing without delay and without prior notice The framework in general lacks some of the details that R6 requires, such as designation criteria set by the UNSCRs and other details that should be in place, which also impact on compliance. Because of the limitations in scope, not all types of assets are covered. However, the provisions of the Counter Terrorism Law contain designation and freezing provisions that despite the above deficiencies allow for R.6 to be partially compliant.

.

[illegible]

Criterion 7.1 There is no general legal basis for designations of UN listed persons or entities. There is also no legal basis for freezing of assets and for a prohibition, except for a freezing requirement for reporting entities mentioned under c.7.2.a; but these measures do not allow for implementation without delay.

Criterion 7.2 The competent authority for the relevant UNSCRs is the MFA.

c.7.2a There is no requirement for all natural and legal persons within the country to freeze without delay and without prior notice, the funds or other assets of designated persons (i.e. a prohibition). For FIs and designated DNFBPs, the PBC has issued Notice 2017/187 which requires the immediate (same day) freezing of assets of designated persons and entities upon instruction of the PBC. The authorities did not establish that such legal orders are issued after issuing of a UNSCR or amendment to the list of designated entities.

c.7.2b. There is no legal requirement to freeze assets that extends to all assets of a designated person or entity. For FIs and designated DNFBPs, the PBC has issued Notice 2017/187, which includes a definition that seems to cover all assets.

c.7.2c
required by R.7.

c.7.2d Not all UNSCRs and UNSC designations are communicated to the financial sector and DNFBPs immediately upon taking such actions. However, the PBC maintains a website with links to UNSCRs (and FATF warnings) and circulates UNSCRs, but this is not systematically done and does not cover every UNSCR and amendment to the list. CDD requirements (see R.10) require banks to use software that include sanctions lists.

c.7.2e. PBC Notice 2017/187 (Arts. 1 and 2) requires reporting of freezing actions by FIs and DNFBPs to the PBC. The only shortcoming in this regard relates to the scope of the financial institutions and DNFBPs that are covered under the AML Law.

c.7.2f. Persons that receive assets from designated entities in good faith acquire property rights, as provided for by the Property Law (Arts. 4 and 106). It is not clear

if such transfers of property titles require UN authorisation, as required by the UN. There are no other provisions to protect bona fide third parties (such as of parties to existing contracts with designated entities)

Criterion 7.3 – PBC Notice 2017/187 (Art. 8) designates the PBC and other financial regulatory authorities to monitor compliance with R.7. The shortcoming in this regard relates to the scope of the sectors that are covered under the AML Law and the range of available sanctions. Authorities report only being able to issue warnings, and fines ranging from RMB 50 000 to RMB 2 million (approx. USD 7 338 to 293 521) (PBC Law Art. 46). See analysis of sanctions for reporting entities R.35.

Criterion 7.4

c.7.4a & b. (7.4.a; (7.4.b – PBC Notice 2017/187 in Art. 5 contains a provision that reporting entities shall inform their customers of the possibility to ask for humanitarian exemptions and for review of the designation by the UN. However, regarding the Focal Point (UNSCR 1730), this legal reference is insufficiently specific. The same shortcoming applies regarding the exemptions under UNSCR 1718 and 1737, which are also not specified in law. Finally, both provisions only assist customers of reporting entities, whereas the review and exemption should be available for all designated entities and applies in very concrete cases (see paragraphs 10 and 11 of INR 7). Finally, there is no legal provision or a procedure to ensure compliance with the notification provision of UNSCR 1737 (or any information that such provisions have in practice been complied with).

c.7.4c. – Publicly known procedures to handle so called false positives are in place, but only apply to those sectors that are designated under the AML Law (PBC Notice 2017/187, Arts. 3 and 4)

c.7.4d – De-listing and unfreezing communications suffer from the same deficiencies as designation/freezing communications (see c.7.2.d), and there is no guidance on how to handle such events

Criterion 7.5 – The MFA is said to have issued notices on implementation of UNSCRs 1718 and 2231 and included specific provisions to cover c.7.5.a and c.7.5.b, and the language is said to track the language of the criterion. However, said Notices were not provided.

Weighting and Conclusion

There are no legal provisions that prohibit legal persons and entities from making funds available to designated entities (i.e., a prohibition). The freezing requirements in Notice 187/2017 are incomplete in scope and only apply to FIs and designated DNFBPs, and the legal provisions do not allow for freezing without delay and without prior notice. The framework in general lacks some of the details that R.6 requires, such as designation criteria set by the UNSCRs and other details that should be in place, which also impact on compliance mechanism. Because of the limitations in scope, not all types of assets are covered.

Recommendation 8 – Non-profit organisations (NPOs)

In the Third Round, China was rated largely compliant on SR.VIII (now R.8). The primary shortcomings identified were a lack of outreach specific to the risk of TF abuse and a supervision and monitoring regime that did not specifically address potential vulnerabilities to terrorist activities, or discovering and preventing possible terrorist threats of misuse of the sector by terrorist financiers. Since the Third Round, R.8 has been significantly amended.

500 social organisations comprised of social groups (368 000), foundations (6 500), and social services institutions (private non-enterprise units) (425 000) as well as 1 227 separately regulated overseas non-government organisations. The Ministry of Civil Affairs (MCA) has the responsibility for the registration and oversight of social organisations while the MPS has the responsibility for the registration and oversight of overseas non-government organisations. These organisations employed a total of 7.637 million people and total contributions and donations for the year amounted to RMB 78.7 billion (approx. USD 11.5 billion). The Š ƒ ” ‹ – › ƒ ™ ‘ ^ – Š ‡ ‡ ‘ ’ Ž ‡ ï • came into effect in 2016 Š ‹ • ƒ and China started the process of registering social organisations as charities. As of June 2018, China had registered 4 194 organisations, the majority (3 265) of which are foundations. Only 992 of the organisations registered as charities to date are permitted to raise funds directly from the public.

Criterion 8.1

c.8.1a According to China, their NRA process used information from supervisors, tax, intelligence, law enforcement, and civil affairs departments to identify the types of NPOs based on their activities or characteristics, that are likely to be at risk of TF abuse. The information presented in the NRA however only covers the inherent risk faced by social organisations and does not attempt to identify a subset of NPOs that fall within the FATF definition of an NPO nor how they identified the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of TF abuse.

c.8.1b While China identified foundations and overseas NPOs as being at higher risk of TF abuse, no information was provided to identify the nature of threats posed by terrorist entities to these types of NPOs nor how they are specifically vulnerable to terrorist actors.

c.8.1c (Partially met) While China has examined its broader NPO sector and taken steps through provisions in the Charity Law to ensure transparency of the sector, it has not demonstrated that it has reviewed the adequacy of measures, including laws and regulations, that relate to the subset of the NPO sector that may be abused for TF support in order to be able to take proportionate and effective actions to address the risks identified.

c.8.1d The PBC and the Ministry of Civil Affairs jointly issued the Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social Organisations, which stipulates that the PBC and its branches and civil affairs departments assess the ML/TF risks of social organisations periodically.

Criterion 8.2 The observations below concern all NPOs, not those that are at risk for TF. The general lack of targeted measures to mitigate TF risks is a shortcoming in itself.

c.8.2a China's Charity Law and the Law on the Administration of Activities of Overseas Non-Governmental Organisations within the Territory of China, along with their relevant regulations, outline the policies promoting accountability, integrity, and

overseas NPOs. The focus of the laws and regulations are on internal governance, fund management, information disclosure and supervision.

c.8.2b The Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social Organisations stipulates that NPOs should take countering TF measures and that the PBC, in conjunction with civil affairs departments, should undertake public educational and training programs to remind NPOs of the risk of TF, and communicate with NPOs to raise awareness of TF risks and appropriate anti-terrorism financing measures. No information; however, was provided with respect to how outreach is conducted nor how China raises awareness of the donor community about the potential vulnerabilities of NPOs to TF abuse and TF risks. While there are websites such as ones operated by the China Social Organisation and Charities in China which disclose information on NPOs and related policies, no information specifically related to the vulnerabilities of NPOs to TF abuse and TF risks is offered.

c.8.2c Art. 22 of the Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social Organisations stipulates that PBC and the civil affairs departments should jointly issue guidance documents about the

organisations and other practices. However, no information was provided regarding the development and refinement of best practices to address terrorist financing risks and vulnerabilities.

c.8.2d Art. 7 of the Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social Organisations stipulates that NPOs should conduct financial transactions through legal financial channels or in a legal manner. Art. 22 of the Law on the Administration of Activities of Overseas Non-Governmental Organisations within the Territory of China outlines similar requirements.

Criterion 8.3 All NPOs are subject to annual inspections by civil affairs departments. These inspections however do not include components related specifically to monitoring for TF abuse. The Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social Organisations provides the PBC with the authority to carry out supervision and inspection on NPOs regarding fulfilling their AML/CFT obligations. To date no such supervision has taken place and it is unclear as to why China would impose AML/CFT obligations on NPOs. The Recommendations do not require this.

Criterion 8.4

c.8.4a The PBC is responsible for the national AML and anti-terrorist financing supervision of NPOs. Civil affairs departments are to cooperate with the PBC by supervising NPOs in their AML and anti-terrorist financing work. However, no

information was provided to indicate that any risk-based supervision is being conducted in respect of TF risks. There have been no specific evaluation criteria developed for the risk of TF abuse and no risk-based strategy developed to prioritise examinations in this regard.

c.8.4b The PBC and civil affairs departments have a range of sanctions available to them for violations of laws and regulations related to the operations of NPOs. The PBC can sanction NPOs with fines ranging from RMB 50 000 (approximately USD 7 339) for directors, to a fine of five times the amount of illicit proceeds for the NPO. Sanctions under the Charity Law include warnings, confiscation, orders to rectify, and fines up to RMB 200 000 (approx. USD 29 352). The public security agencies equally can impose sanctions according to different illegal activities of the overseas NPOs, including: banning or ordering to stop the illegal acts; confiscation of illegal property and illegal income; revoking or temporarily banning the registration and certificates; and giving a warning to the directly responsible personnel, and in serious cases, 10 15 days detention. China implements a bipartite punishment system, where sanctions can be imposed on both the NPO and persons acting on behalf of an NPO. Given the range of sanctions available and the bipartite punishment system available to Chinese authorities, these sanctions would be considered effective proportionate and dissuasive

Criterion 8.5

c.8.5a (Met) Art. 17 of the Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social

c.8.5d Art. 17 of the Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social Organisations indicates that where the PBC and civil affair authorities have reasonable grounds to suspect that social organisations are involved in criminal activities such as ML and TF, they shall report to public security and notify each other.

Criterion 8.6 Art. 20 of the Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Social Organisations indicates that relevant information obtained from NPOs by the PBC and civil affairs departments can be used for international cooperation.

Depending on the source of the requests and the nature of information or assistance requested, China will respond to international requests through appropriate authorities and procedures. Requests are handled as follows: (i) judicial MLA is provided through the MoJ or the SPP according to relevant agreements; (ii) police cooperation is provided through the MPS; (iii) financial intelligence exchange is provided by CAMLMAC; and (iv) other international cooperation requests may be channelled through the MFA. Each department has established its own procedures for receiving, assessing, and responding to these types of requests.

Weighting and Conclusion

Through the various laws that pertain to Social Organisations and Overseas Non-Governmental Organisations, China is able to ensure a decent level of transparency, and accountability, integrity and public confidence in its broader NPO sector. The 2016 Š ƒ ”‹–› ƒ™ ‘ – Š ‡ ‡‘ Ž ‡ï • with it strengthened this situation. China however has not attempted to identify the subset of organisations within its broader NPO sector in an effort to identify those organisations that meet the FATF definition of an NPO and are therefore at risk of TF abuse. China does not have a risk-based monitoring mechanism to address the risk of TF within this sector and has not demonstrated that it conducts outreach specific to the risk of TF abuse.

General Information on Preventive Measures of the Financial Sector

Regulations applicable for FIs do not cover payment institutions. The latter entities have their own AML/CFT regulations. General information is provided in the following Recommendations.

[illegible]

In its previous MER, China was rated compliant with the former R.4.

Criterion 9.1 While the ƒ ™ ‘ ˆ – Š ‡ ‡‘ Ž ‡ï • ‡’ — „ Ž ‹ … ‘ ˆ Š ‹• ƒ • ‘•• ‡” … and the Securities Law include provisions that require customer information to be kept confidentially, several laws and regulations provide supervisors and LEAs wide ranging powers to override these provisions and gain access to such information. These include the ƒ ™ ‘ ˆ – Š ‡ ‡‘ Ž ‡ï • ‡’ — „ Ž ‹ … ‘ ˆ Š ‹• (Arts. 61 ‘•• ‡” … ‹ƒ Ž and 62), – Š ‡ ‡ … — ” ‹ – ‹ • ƒ ™ (Republic of China (Arts. 148, 180, and 183), – Š ‡ •• — ” ƒ • … ‡ ƒ ™ ‘ ˆ – Š ‡ ‡‘ Ž ‡ï • (Art. 150), the Criminal Procedure ƒ

Law (Art. 52), and Measures for the Administration of AML/CFT of Payment Institutions (Arts.
China (Art. 35) provides for the establishment of a mechanism for the sharing of information among financial sector supervisors and the AML Law provides that customs and other government agencies which undertake AML functions shall report any suspicious transactions to the investigative authorities. FIs are required to provide supplementary information to the CAMLMAC when requested to do so (Art. 28, Measures for the Admin• – ” ƒ – ‹ • ‘ ^ ‹ • ƒ • … ‹ ƒ Ž • • – ‹ – — – ‹ ‘ • • ï ‡ ’ ‘ ” – ‹ • ‰ ‘ ^ Transactions and Suspicious Transactions). The AML Law (Art. 28) also provides for the sharing of information with foreign governments. FIs are required to provide customer and transaction information to intermediary and beneficiary institutions (Art. 10 of Administrative Measures for Customer Identification and Documentation of Customers Identity Information and Transaction Records by Financial Institution 2007 (2). Art. 1 (1) of the Notice of the Peoples Bank of China on Strengthening the Anti Money Laundering in Cross Border Remittances PBC Documents No 2012 (199). There are no legal provisions which address the sharing of information within financial groups, but such institutions can share information in accordance with the laws and regulations discussed above.

Weighting and Conclusion

[illegible]

In its Third Round MER, China was rated partially compliant with the former R.5 on CDD (see 3.2.3). Main shortcomings were the lack of CDD obligations for beneficial owners, lack of enhanced and ongoing due diligence obligations, lack of specific requirements for the identification of legal persons (except for banks), lack of obligation to determine whether the customer is acting on behalf of another person, undetermined threshold for the implementation of CDD for occasional transactions, and the lack of effectiveness. The CDD recommendation has been strengthened with the revision of FATF standards in 2012.

Due diligence measures for FIs providing safety deposit box services, are limited to Art. 9 of Administrative Measures for Customers Identification and Documentation of Customers Identity Information and Transaction Records by Financial Institutions).

Criterion 10.1 FIs Art. 16 of AML Law).

Criterion 10.2

c.10.2 a c FIs should, when establishing any business relationship with a client or providing occasional transactions above a designated threshold, require the client to certificat Art. 16 of AML Law). Art. 7 of Administrative Measures for Customers Identification and Documentation of Customers Identity and Transaction Records by Financial Institutions (Order of the PBOC, CSRC, and CIRC No. [2007] 2) sets a threshold of RMB 10 000 or

foreign currency with equivalent value of USD 1 000[69] for a single sum of occasional transactions (such as cash remittance, cash exchange, negotiable instrument cashing) and requires institutions to get information about the natural person(s) who ultimately controls a customer and/or the natural person on whose behalf a transaction is being conducted.

Payment institutions should complete the identity verification of the customer and its beneficial owner before establishing a business relationship or conducting occasional transactions above the designated threshold (Art. I.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • Bank of China Notice on Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD [2018] 130)). However, payment institutions are not required to undertake CDD measures when carrying out occasional transactions in several operations that appear to be linked for a total exceeding the equivalent of USD/EUR 15 000.

c.10.2(d-e) When there is a suspicion of ML/TF, FIs, including payment institutions, - -identification is also required when the institution has doubts about the veracity or adequacy of previously obtained customer identification data (Art. 22 of Administrative Measures for Customers Identification and Documentation of Customers Identity and Transaction Records by Financial Institutions (Order of the PBC, CSRC, and CIRC No. [2007] 2))

Criterion 10.3 Financial institutions, including payment institutions, should identify and verify the identity of customers using reliable, independent source documents, data or information. These measures apply to all customers whether permanent and occasional, and to customers that are natural or legal persons or legal arrangements (Art. 3 of AML Law; Art. I.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD [2018] 130)).

Criterion 10.4 FIs should identify and verify the identity of any person purporting

(Art. 16 of AML Law; Art. 20 of Administrative Measures for Customers Identification and Documentation of Customers Identity and Transaction Records by Financial Institutions (Order of the PBC, CSRC, and CIRC No. [2007] 2)). Prepaid card institutions are required to verify, when a proxy buys a prepaid card on behalf of others, the existence of the proxy relationship through a reasonable manner and identify and verify the identity of the proxy. No such requirements for other types of payment institutions exist (Art. 15 of Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Payment Institutions (PBC Document No. [2012] 54)

Criterion 10.5 FIs
person(s) who ultimately controls a customer and/or the natural person on whose

beneficial owner of the non-natural person clients and trace down to the natural person who ultimately controls or owns the be
definition of beneficial owner is qualified as it referring to a natural person who

69 Which falls below the applicable designated threshold of (USD/EUR 15 000) for occasional transactions in the FATF standards.

is no explicit requirement for payment institutions to ensure that documents, data, or information collected under the CDD process is kept up-to-date and relevant.

Criterion 10.8
understst -natural-

-natural-
In this process they must collect, understand, and preserve registration certificates, proof of existence, the partnership agreement, the trust agreement, memorandum and articles of association and registration information of shareholders or members of the board (including the board of directors, senior management and list of shareholders, number of shareholdings of each shareholders and ownership types (including related voting type)) (Arts. 1.1 and 1.8 of Notice of the PBC on Strengthening Customer Identification Mechanism in AML (PBC Document No. [2017] 235). However, the requirement to implement these measures seems to be unduly limited to taking reasonable measures.

Criterion 10.9 Regulated institutions should understand, obtain, and properly retain the following information and materials on non-natural-person clients: ownership of shares or right of control (mainly includes: registration certificates, proof of existence, the partnership agreement, the trust agreement, memorandum and articles of association), registration information of shareholders or members of the board (mainly includes: the board of directors, senior management and list of shareholders, number of shareholdings of each shareholders and ownership types (including related voting type etc.). Financial institutions are also required, among other information, to register the address; scope of business; the name, number, and valid term of the license, certificate, or document which may prove that the client is lawfully established or lawfully carries out the business operation or social activities; the names of the legal representative, person in charge and authorised working

For payment institutions, the veri
occur through similar information (Art. 1.8 of Notice of the People's Bank of China on Strengthening Customer Identification Mechanism in Anti-Money Laundering (PBC Document No. [2017] 235), Arts. 7 and 33 of Administrative Measures for Customers Identification and Documentation of Customers Identity and Transaction Records by Financial Institutions (Order of the PBC, CSRC, and CIRC No. [2007] 2), Art. 51 of Measures for the Administration of Anti-

Notice on Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD [2011] 130)). However, FIs are not required to take enhanced measures, beyond enhanced customer identification measures, if it determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk.

Criterion 10.14 FIs, including payment institutions, are required to verify the identity of the customer when establishing a business relationship (Art. 16 of AML Law) Art. I.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ ‘ – ‹ … ‡ Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD [2018] 130) stipulates that

complete the identity verification of the customer and its beneficial owner before establishing a business relationship or conducting occasional transactions above the designated threshold, and are permitted to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the ML/TF risks are effectively managed and where this is essential not to interrupt the normal conduct of business. should establish corresponding risk management mechanisms and procedures to implement effective risk management measures with respect to the conditions under which a customer may utilise the business relationship prior to verification, such as limiting the number of transactions, type or amount of transactions, and strengthening transaction monitoring.

Criterion 10.15 Regulated institutions are required to establish corresponding risk management mechanisms and procedures to implement effective risk management measures with respect to the conditions under which a customer may utilise the business relationship prior to verification, such as limiting the number of transactions, types or amount of transactions, and strengthening transaction monitoring (Art. I.1 of Notice ‘ ˆ – Š ‡ ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Further Strengthening Anti-Money Laundering and Countering Terrorism Financing (PBC GAD [2018] No. 130)). However, financial institutions may allow low-risk customers only to utilise the business relationship prior to verification, provided that risks are controllable (Art. IV.II.1 of Notice of the PBC on Issuing the Guidelines for the Assessment of ML/TF Risks and Categorized Management of Customers of Financial Institutions (PBC Document No. [2013] 2)). Given that Art. I.1 of (PBC Document No. [2013] 2) stipulates that its implementation is not mandatory, the requirements governing the situation where low-risk customers are allowed to utilise the business relationship prior to verification are not clear.

Criterion 10.16 FIs are required to supplement or update CDD information of existing customers (Art. II.1 of Notice of the PBC on Further Strengthening the AML Work of Financial Institutions (PBC Document No. [2008] 391)) and are expected to enhance the updating of records when risks are high. However, it is not provided that updating should be performed on the basis of materiality or at appropriate times.

Payment institutions are required to complete CDD information of existing customers within two years (General provisions of Measures for the Administration of Anti-Money Laundering and Combating the Financing of Terrorism of Payment Institutions (PBC Document No. [2012] 54)). The implementation of CDD for existing relationships of

payment institutions is not required on the basis of materiality and risk, and at appropriate times.

Criterion 10.17 Art. II.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD 2018 130) stipulates that, in situations where the ML/TF risk

and transaction monitoring measures commensurate to the risks. The Article also provides for a series of enhanced measures that can be taken by institutions commensurately to risk. However, Art. I.1 of (PBC Document No. [2013] 2) stipulates that its implementation is not mandatory, therefore, it is not clear whether or not it is mandatory for financial institutions to apply enhanced measures in situations where ML/TF risks are high.

Criterion 10.18 FIs should scientifically allocate AML resources according to the risk assessment results and adopt simplified AML measures in areas with lower ML risks. For customers with significantly lower risks that can be effectively controlled, an FI may, at its discretion, decide to directly assign the lowest risk level to them (without assessment), provided that some circumstances[72] do not apply, including that the customer is involved in any report on suspicious transactions (Art. I.1.1, II.IV.1 of Notice of the PBC on Issuing the Guidelines for the Assessment of ML/TF Risks and Categorized Management of Customers of Financial Institutions (PBC Document No. [2013] 2). However, Art. I.1 of (PBC Document No. [2013] 2) stipulates that its

transaction reports, if ther

Criterion 12.2 For senior management of international organis

the Notice of the PBC on Strengthening Customer tidea tion Mechanism in AML (PBC Document No. [2017] 23), when encountering higher risk in providing services (Art. 2.2 of Notice of the PBC on Strengthening Customer Identification Mechanism in AML (PBC Document No. [2017] 23). However, financial institutions are not required to implement specific due diligence requirements for domestic PEPs.

Criterion 12.3 Financial institutions are required to perform the obligation of due

p

otherwise closely related to them (Art. 2.4 of Notice of the PBC on Further Strengthening the AML Work of Financial Institutions (PBC Document No. [2008] 391). Specific natural persons such as foreign PEPs and senior executives of international organisations including foreign PEPs, senior management personnel of international organisations, as well as close relatives including parents, spouses, children, etc., as well as other natural persons who have a relationship of generating and sharing common interests through work and life that the regulated institutions know or should know (Art. 4.2 of Notice of Further Strengthening Work on the Identification of Beneficiary Owners (PBC Document No. [2018] 164)). However, these requirements do not apply for domestic PEPs.

Criterion 12.4 Generally, where risk level is hi2 (and 0 595.32 .47 Td [(Bener3.99412.002 (n)4-4

In the Third Round, China was rated largely compliant with the former R.17, due mostly to inadequate sanctions, and sanctions not focusing on structural weaknesses.

Criterion 14.1 In China, commercial banks are permitted to engage in the business of MVTS under their banking licenses. Non-bank FIs must obtain a Payment Business Permit following an approval process by the PBC (Measures for the Administration of Payment Services of Non-Financial Institutions, Art. 3). This measure is not applicable to natural persons. Involvement of natural persons in remittance activity is a criminal offence (Art. 255, Criminal Law).

Criterion 14.2 It is a criminal offence to engage in fund payment and settlement activity is a a -3.995 (

Weighting and Conclusion

Arrangements are in place to ensure that MVTS providers are licensed and monitored for AML/CFT compliance. Banks are not explicitly required to include agents in their AML/CFT programs and monitor them for compliance with such programs.

.

[illegible]

In its previous MER, China was rated largely compliant with the former R.8. The main deficiency identified was the absence of requirements related to non-face-to-face business in the insurance sector.

Criterion 15.1
by various types of FIs. It examines risks associated with some newer products/services such as prepaid cards, online lending services (e.g. peer-to-peer loans).

Financial institutions are required to analyse risks of their financial business and marketing channels, especially before launching any financing business, marketing channel, or new technology. Art. 2, Chapter 5 of The Notice of the PBC on Issuing Guidelines for the Assessment of ML/TF Risk and Categorized Management of Customers of Financial Institutions

that PIs have been sanctioned for violation of these provisions; however, there is no explicit requirement for PIs to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices.

Criterion 15.2 Financial institutions are required to analyse risks arising from its financial business and marketing channels, especially before launching any financing business, marketing channel or new technology. They are also required to develop appropriate measures to adequately mange risks identified (Chapter 5, Art. 2 of The Notice of the PBC on Issuing Guidelines for the Assessment of ML/TF Risk and Categorized Management of Customers of Financial Institutions. See comment on payment institutions in 5.1).

Weighting and Conclusion

While FIs are required to identify and assess risk in relation to the development of new products and take appropriate measures to mitigate such risks, PIs, which offer many innovative products, are not subject to such obligations.

.

[illegible]

In its previous MER, China was rated largely compliant with the former SR.VII. The main deficiency identified was that customer verification was only required for payments in excess of the equivalent of USD 1 300. The FATF standards in this area have since expanded to include requirements related to beneficiary information.

Criterion 16.1 Financial institutions providing cross-border remittance services, including wire transfers,

Where an account number cannot be obtained for either the originator or the beneficiary, the institution must use a unique transaction reference number that allows the transaction to be traced Notice on Further Strengthening Work on Anti Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018) 130). In the case of cross-border transfers of RMB10 000 or a foreign currency transfer equivalent to USD1 000, institutions must verify the originator information. (Art. 1 (1) of the ‘–‹…‡‘ˆ–Š‡‡‘Ž‹•Š‡–•‘ˆ–Š‡ Remittances (PBC Document 2012 (199). As RMB10 000 is equivalent to approximately USD1 467,[75] there is no obligation to verify originator information obtained on cross-border transfers denominated in yuan unless the amount of the transfer exceeds the yuan equivalent of USD1 467.

Criterion 16.2 (Not applicable) There are no specific requirements for batch transfers. Such transfers must therefore comply with the provisions described under c.16.1.

Criterion 16.3 It is a requirement that the information set out under 16.1 accompany all wire transfers (Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018) 130). For cross border transfer under RMB 10,00 USD 1,467 such information would not be verified Regulated

Criterion 16.4 In the case of cross-border transfers of RMB10 000 or a foreign currency transfer equivalent to USD1 000, institutions must verify the originator information. (Art. 1 (1) of the ‘–‹…‡‘ˆ–Š‡‡‘Ž‹•Š‡–•‘ˆ–Š‡ AML in Cross Border Remittances (PBC Document 2012 (199). As RMB10 000 is equivalent to approximately USD1 467,[76] there is no obligation to verify originator information obtained on cross-border transfers denominated in yuan unless the amount of the transfer exceeds the yuan equivalent of USD1 467. These provisions do not include an obligation to verify beneficiary information. Where there is suspicion of ML or other illegal activity, regulated institutions are required to verify the identity of the originator but not the beneficiary. Art. II (1) of the Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018) 130, equivalent of USD1 000, there is, therefore, no

Criterion 16.5 The legal requirements applicable to domestic wires transfers relate

Measures for Payment and Settlement PBC Document (1997), 393 provides that a

name and account number of the originator, and the beneficiary. The bank must reject a remittance certificate that does not include this information. There is no requirement for the information to be verified. In addition, this requirement is applicable to banks and not to other institutions that provide domestic wire transfer services. There is no provision that would allow this information to be made available

75 Based on RMB/USD exchange of 6.8138 as at July 27, 2018 the last day of the onsite.

76 Based on RMB/USD exchange rate of 6.8138 as at July 27, 2018, the last day of the onsite.

to the beneficiary financial institution or appropriate authority through other means. Payment institutions are required to ensure that all transactions include the name

identification number. There is no requirement for the information to be verified. There is no provision that would allow this information to be made available to the beneficiary financial institution or appropriate authority through other means

Criterion 16.6 (Not applicable) There is no provision that would allow information that should accompany a wire transfer to be sent separately from the transfer.

Criterion 16.7 The provisions of Art. 19 of the AML Law which require identification information to be maintained for a period of five years after the end of the business relationship and transaction records to be maintained for five years after the date of the transaction, apply to the information collected on the originator and beneficiary, in the case of wire transfers.

Criterion 16.8 Ordering institutions are prohibited from executing a transfer if it does not comply with the requirements of the 16.1 to 16.7 Art. II (4) (4) Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018). As there is no requirement to verify originator information for cross-border transfers less than RMB 10 000, ordering institutions are not prohibited from executing transfers that do not meet the requirements of R.16.1 16.7 in this regard.

Criterion 16.9 Intermediary institutions are required to ensure that all originators and beneficiary information accompany wire transfers and are retained with it (Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018) 130)).

Criterion 16.10 The provisions of Art. 19 of the AML Law which require identification information to be maintained for a period of five years after the end of the business relationship, and transaction records to be maintained for five years after the date of the transaction, apply to the information collected on the originator and beneficiary, in the case of wire transfers and are applicable to all FIs, including intermediary institutions. In circumstances in which originator or beneficiary information does not accompany the wire transfer, the intermediary institution is required to retain the information received from other institutions.

Criterion 16.11 On receiving funds from abroad, regulated institutions are required to take reasonable measures to identify cross-border wire transfers that lack required originator and beneficiary information (Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018) 130)).

Criterion 16.12 Regulated institutions that are intermediary institutions are

identify cross border transfers that lack required originator and beneficiary information. Art. II (3) Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018).

Criterion 16.14 In the case of cross-border transfers of RMB10 000 or a foreign currency transfer equivalent to USD1 000, beneficiary institutions must verify the beneficiary information (Art. 1 (2) of – Š ‡ ‘ – ‹ … ‡ ‘ ^ – Š ‡ ‡ ‘ ' Ž ‡ ï • f • • ‘ ^ Š ‹ • Strengthening AML in Cross Border Remittances (PBC Document 2012) (199). Payment institutions are not allowed to make cross-border wire transfers. As RMB10 000 is equivalent to approximately USD1 467, there is no obligation to verify beneficiary information related to cross-border transfers denominated in yuan that are below this threshold. Art. 19 of the AML Law requires FIs to maintain information in accordance with R.11.

Criterion 16.15 Where cross-border transfers lack required originator and beneficiary information regulated institutions that are beneficiary institutions are required to have risk-based policies and procedures to determine if it should execute, reject or suspend the transfer and to take follow-up action (Art. II (3) Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018) 130).

Criterion 16.16 This criterion is not applicable to payment institutions as they are not permitted to use agents. However, banks can use agents., Financial institutions are required to ensure that their overseas branches and subsidiaries implement group requirements (see analysis of c.18.3). The deficiencies discussed with regard to R.16 would apply to FIs overseas branches, subsidiaries and agents.

Criterion 16.17 Where a regulated institution that controls both the ordering and the beneficiary side of a wire transfer it is required to review all information from both the ordering and beneficiary sides in determining if an STR should be filed. This requirement does not cover the filing of STRs in any country affected by the suspicious wire transfer (Art. II (4) (3) Notice on Further Strengthening Work on Anti-Money Laundering and Combatting the Financing of Terrorism [PBC GAD] (2018) 130).

Criterion 16.18 Financial institutions, including those providing wire transfer services, are required to take the relevant measures stipulated in notices received from the MFA concerning the implementation of the resolutions of the UNSC. Such measures include freezing accounts and suspending transactions (The Notice of the ‡ ‘ ' Ž ‡ ï • f • • ‘ ^ Š ‹ • f ‘ • • ' Ž ‡ • ‡ • – ‹ • ‰ ‡ ŽU N Security Council – ‹ ‘ • • ‘ ^ – Š ‡ (PBC document (2017) 187)) (see related deficiencies discussed under c.6.5)

Weighting and Conclusion

China has generally sound requirement related to wire transfers. The threshold of RMB equivalent of USD1 467 for verifying the identify of originators and beneficiaries, deficiencies in requirements for an institution that cover both side of a transfer, and weaknesses with respect to targeted financial sanctions are notable weaknesses in the arrangements.

[illegible]

In its Third Round MER, China was rated partially compliant with the former R.9 on reliance on third parties. Main shortcomings were the lack of: (i) requirement to obtain core customer identification data from the third-party; (ii) requirement to ascertain the status of the third party with respect to regulation and supervision for AML purposes, and (iii) conditions in relation to reliance on third parties emanating from countries with inadequate AML regimes.

Criterion 17.1 Chinese laws allow FIs to rely on third parties for performing CDD measures (Art. 17 of AML Law). [illegible]-party institutions to perform customer identification, they shall take following measures: (i) satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, customer identification and record-keeping requirements in line with AML laws, administrative regulations, and the requirements of this notice; (ii) obtain immediately the necessary information of customer identification from the third-party institution; and (iii) take steps to satisfy themselves that copies or photocopies of customer identification documents and other related materials from the third party upon request without delay. The regulated institution should assume the responsibility of the third-party institution for failure to fulfil customer identification obligations (Art. I.2 of General Office of the [illegible] Money Laundering and Combating the Financing of Terrorism (PBC GAD (2018) 130)). However, the provisions do not stipulate what are necessary information that should be obtained immediately from the third-party.

Criterion 17.2 When determining in which countries the third party that meets the [illegible] relying on third parties located in the high-risk countries or regions to carry out customer identification (Art. I.2 of General [illegible] Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD (2018) 130)).

Criterion 17.3 (Not applicable) China does not have specific requirements for FIs that rely on a third party that is part of the same financial group.

Weighting and Conclusion

The only shortcoming is the lack of specific requirement in relation to necessary information that should be obtained from a third-party.

.

[illegible]

In its Third Round MER, China was rated partially compliant with the former R.15 internal controls, and non-compliant with the former R.22 on foreign branches and subsidiaries. Main shortcomings with respect to the former R.15 were the internal control environment is not set up to address TF risk, and the lack of requirements on: (i) communicating policies and procedures to employees; (ii) screening provisions

mechanism to implement counter-measures against countries that did not sufficiently apply the FATF standards. R.19 strengthens the requirements to be met by countries and FIs with respect to higher-risk countries.

Criterion 19.1 FIs, including payment institutions, are required to apply enhanced customer identification measures and on-going transaction monitoring proportionate to the [illegible] areas by the FATF (Notice on Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD [2018] 130) Art.

Weighting and Conclusion

There are conflicting reporting requirements in place for payment institutions. In addition, the minor deficiency regarding the scope of predicate offences for ML, as identified in the analysis of R.3 above, has a spill over on the reporting obligation.

[illegible]

In the Third Round MER, China was rated compliant with these requirements.

Criterion 21.1 Financial institutions, including payment institutions, and their employees "are protected by law" when fulfilling their obligation to report suspicious transactions in accordance with the law (AML Law, Art. 6 and Measures for the Administration of Financial Institutions' Reporting of Large-Value Transactions and Suspicious Transactions, Art. 11). The AML Law does not define the extent of this protection, but the authorities clarified that many other laws contain a similar protection provision. There is jurisprudence that shows that the courts interpret this protection broadly to include both criminal and civil liability.

Criterion 21.2 Tipping off is prohibited under Art. 15 of the Provisions on Anti-Money Laundering Through Financial Institutions and Art. 23 of the Measures for the Administration of Financial Institutions' Reporting of Large-Value Transactions and Suspicious Transactions, which prevent financial institutions, including payment institutions, and their staff from disclosing to their customers, or any other person, information relating to suspicious transactions and any resulting investigation by the PBC. These provisions do not appear to inhibit information sharing under R.18 by FIs with the exception of payment institutions (Notice of the People's Bank of China on Strengthening Customer Identification Mechanism in Anti-Money Laundering, Section 3(5), which does not apply to payment institutions).

Technical compliance

General Information [on preventive measures for DNFBPs]

Authorised trust investment companies are the only entities in China that are permitted to be in the business of administering trusts (Regulations on Trust Investment Corporations issued in 2001 and revised in 2002). No other FIs, lawyers, accountants, or other professionals are permitted to engage in this activity as a business. Trust investment companies are treated as FIs (nonbank banking institutions) under Chinese law, and are supervised by the CBRC. However, authorities stated that the PBC still assumes the AML regulatory responsibilities for trust companies.

Any individual or entity that has obtained authorisation from the administrative departments of the SAMR (the general enterprise registration procedure) can be a company service provider (i.e., someone who is authorised to be in the business of assisting in the establishment or registration of companies). No particular qualifications are necessary in order to obtain such authorisation.

The scope of the DNFBPs that shall perform AML obligations and the specific AML obligations thereof need to be formulated by the PBC in collaboration with the relevant departments of the State Council (AML Law, Art. 35). On July 26, 2018, the Notice of the General Office of the People's Bank of China on Strengthening Anti-Money Laundering Supervision Work on Designated Non-Financial Businesses and Professions, 2018, No. 12 entered into force. This Notice designates the DNFBPs and subjects all DNFBPs to AML/CFT requirements imposed under different regulations for different sectors, invariably. Given that this Notice was not issued in collaboration with the relevant departments of the State Council, the designation is deemed to not be made yet, except for precious metals trading venues (since PBC is the regulator of this sector). The Notice of the MHURD, the PBC, and the China Banking Regulatory Commission on Regulating the Financing of Home Buying and Strengthening Anti-Money Laundering (MHURD Document No. [2017] 152) provided some AML obligations for real estate agents, however, it was not issued based on the AML Law and did not make an explicit designation of real estate agents as DNFBPs. Similarly, the Notice on Strengthening the Supervision of Certified Public Accountants (Ministry of Finance Accounting Department Document No. [2018] 3) includes AML/CFT obligations (internal control system, CDD, record-keeping, and carrying out enhanced due diligence according to risk assessment result and reporting suspicious transactions) for accountants. In the absence of a designation, DNFBPs are therefore not subject to AML/CFT obligations, except for precious metals trading venues. In addition to relevant provisions in the AML Law, the Notice of the PBC on Strengthening the Anti-Money Laundering and Combating the Financing of Terrorism Related to Precious Metals Trading Venues (PBC Document No. [2017] 218) provides AML obligations for precious metals trading places (Thereafter, DPM: Dealers in Precious Metals). The PBC required the forwarding of this Notice to members and their agents, therefore, it is considered that the Notice is only enforceable for trading places and dealers.

The PBC is working with competent departments of relevant industries to establish the AML/CFT administration systems for lawyers and notaries, which will stipulate obligations on CDD, record-keeping, PEPs, new technologies, internal controls, enhanced CDD measures against the higher-risk countries, and tipping-off and confidentiality for these DNFBPs.

Criterion 22.1 DPM should establish and improve a clients' identity identification system (Art. 3 of AML Law). When conducting customer identification, DPMs verify the identity of customers using reliable, independent source documents, data or information, and understand and, as appropriate, obtain information on the purpose and intended nature of the customer's establishment and maintenance of the business relationship. DPMs should also complete the identity verification of the customer and its beneficial owner before establishing a business relationship or conducting occasional transactions above the designated threshold and are permitted to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the ML/TF risks are effectively managed and where this is essential not to interrupt the normal conduct of business. DPMs should establish corresponding risk management mechanisms and procedures to implement effective risk management measures with respect to the conditions under which a customer may utilise the business relationship prior to verification, such as limiting the number of transactions, type or amount of transactions, and strengthening transaction monitoring (Art. 3 of AML Law; Art. I.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • Bank of China Notice on Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD 2018 130)). DPMs should understand the natural person(s) who ultimately controls a customer and/or the natural person on whose behalf a transaction is being conducted. (Art. II.1 of Notice of – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ – ”-‡ • Money Laundering and Combating the Financing of Terrorism Related to Precious Metals Trading Venues (PBC Document No. [2017] 218). However, there is no explicit requirement to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner, using the relevant information or data obtained from a reliable source, such that the DPM is satisfied that it knows who the beneficial owner is.

DPMs should conduct ongoing customer identification measures on the business relationship, review in detail the recorded customer data and transactions occurred during the existence of the business relationship, update customer identification documents, data, information, and materials in a timely manner to ensure that the

customer, their business and risk profile, including where necessary, the source of funds. For higher-risk categories of customers, DPMs should increase the frequency and intensity of the on-going monitoring (Art. I.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • of China Notice on Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD 2018 130)). However, there is no explicit requirement for DPM to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant.

Art. II.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ – ‹ … ‡ ‘ • — ”- Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD 2018 130) stipulates that, in situations where the ML/TF risk is higher, DPMs should take appropriate customer identification and transaction monitoring measures commensurate to the risks. The Article also provides for a series of enhanced measures that can be taken by DPMs commensurately to risk.

e to or have trade with any client who cannot clarify his identity (Art. 16 of AML Law). If DPM are unable to comply with relevant

customer identification work or after an assessment that the circumstances exceed the risk management capabilities of the institution, it shall not establish or maintain business relationships with the customer and shall consider submitting an STR in relation to the customer (Art. I.1 of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ on Further Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD 2018 130)).

There are no obligations for DPMs stipulating situations when CDD is required. DPMs are not required to (i) verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person; and (ii) apply any specific CDD measures for legal persons and arrangements. In addition, DPM are not permitted not to pursue the CDD process (and required to file an STR) in cases where a ML/TF suspicion is formed, and they reasonably believe that performing the CDD process will tip-off the customer.

Requirements for TSPs are the same as those for FIs, and, therefore, the analysis under R.10 applies here for TSPs. The other DNFBPs are not designated yet; therefore, they are not subject to CDD requirements.

Criterion 22.2
transaction records for at least five years, and ensure that they can reconstruct every transaction precisely and completely (Art. II.e of ‘ – ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ on Strengthening the Anti-Money Laundering and Combating the Financing of Terrorism Related to Precious Metals Trading Venues (PBC Document No. [2017] 218) DPMs should have programs to ensure that all customer identity information and transaction records are available swiftly, conveniently and accurately to domestic competent authorities including regulatory authorities and LEAs upon appropriate authority (Art. V of General Office of – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ ‘ – ‹ … ‡ ‘ • — ” Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD 2018 130)). However, the requirement to keep records for five years does not specify as of when it should start to apply. The requirement to keep transaction records does not extend to business correspondence and results of any analysis undertaken.

Requirements for TSPs are the same as those for FIs, and therefore the analysis under R.11 applies here for TSPs. The other DNFBPs are not designated yet; therefore, they are not subject to CDD requirements.

Criterion 22.3 Requirements for TSPs are the same as those for FIs, and, therefore, the analysis under R.12 applies here for TSPs. The other DNFBPs are not designated yet; therefore, they are not subject to CDD requirements.

Criterion 22.4 Requirements for TSPs are the same as those for FIs, and therefore the analysis under R.15 applies here for TSPs. The other DNFBPs are not designated yet; therefore, they are not subject to CDD requirements.

Criterion 22.5 If DPM rely on third-party institutions to perform customer identification, they shall take following measures: (i) satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, customer-identification and record-keeping requirements in line with AML laws, administrative regulations and the requirements of this notice; (ii) obtain immediately the necessary information of customer identification from the

suspect that funds are the proceeds of a criminal activity; or (ii) attempted transactions. Moreover, the obligation to report suspicion is not set in a law.

DPMs should promptly submit the reports to the CAMLMAC and the PBC or its local branches (Art. V. of ‡ • ‡ ” ƒ Ž ˆ ˆ ‹ … ‡ ‘ ˆ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ƒ • • ‘ ˆ Š ‹ • ƒ ‘ – ‹ … ‡ Strengthening Work on Anti-Money Laundering and Combating the Financing of Terrorism (PBC GAD 2018 130)).

Requirements for TSPs are the same as those for FIs, and, therefore, the analysis under R.20 applies here for TSPs. The other DNFBPs are not designated yet; therefore, they are not subject to CDD requirements.

Criterion 23.2 Requirements for TSPs are the same as those for FIs, and, therefore, the analysis under R.18 applies here for TSPs. The other DNFBPs are not designated yet; therefore, they are not subject to CDD requirements.

Criterion 23.3 Requirements for TSPs are the same as those for FIs, and, therefore, the analysis under R.19 applies here for TSPs. The other DNFBPs are not designated yet; therefore, they are not subject to CDD requirements.

Criterion 23.4 When a DPM submits a report on a suspicious transaction, it shall be protected by law (Art. 3 of AML Law). There are no law provisions (i) providing a similar protection for directors, officers and employees of a DPM from both criminal and civil liability; (ii) prohibiting those from disclosing the fact that an STR or related

34, 36 37, 63 64, and 68). Additional similar measures are in place specifically for listed companies (Securities Law, Arts. 20, 63, 67, 160, and 193). The verification of the registered information is undertaken through a random check (Art. 2, of the Interim Measures for the Random Inspection of Public Disclosure of Information by Enterprises), but there are no other mechanisms to ensure accuracy and timely updating of the information referred to in 24.3 and 24.4.

Criteria 24.6 and 24.7 Beneficial ownership information is not required nor registered at company formation stage, or to by the companies themselves. To comply with this criterion, authorities refer to the existing information obtained by FIs. However, financial institutions only need to take reasonable measures to identify the beneficial owner and monitor CDD information for accuracy, but there is no requirement regarding timeliness. No beneficial ownership information would be available on companies (or specific entities that are part of larger legal structures) or other types of legal entities that are not a customer of a financial institution in China.

Criterion 24.8 The are no specific additional requirements to ensure that companies cooperate with competent authorities to the fullest extent possible to determine the beneficial owner.

Criterion 24.9 Basic ownership information collected at creation and information on directors and board must be kept indefinitely by the company (Provisions on the Scope of Collection and Preservation Period in the Document Archiving of Enterprises Art. 8.1) and upon dissolution of the entity sent to the SAMR (Archives Law, Art. 11 and SAIC Archive Measures, Arts. 5 and 6). No beneficial ownership information is collected or maintained, but if beneficial ownership information was collected as part of CDD, then it must be kept for five years after the end of the business relationship (see R.11).

Criterion 24.10 Basic legal ownership information (as far as collected) is publicly available, as noted under criterion 24.1. No beneficial ownership information is collected or maintained, but if beneficial ownership information was collected as part of CDD then law enforcement bodies have the powers to obtain basic legal ownership information as part of their regular coercive powers (see R.31) from FIs and financial supervisors can obtain the information also as part of their regular supervisory powers (see R.27), but sharing is not given.

Criterion 24.11 Bearer shares are permitted to be issued by all domestic and foreign registered companies that issue shares. Transfer of bearer shares becomes effective immediately upon delivery of the shares by the shareholder to the transferee. Transfer of shares by shareholders must be conducted at a securities trading place established according to the law or by other means as stipulated by the State Council (Company Law, Arts. 129, 138, and 140). In practice, this means electronic (dematerialized) transfer of shares through the China Securities Depository and Clearing Corporation (CSDC), which is also the custodian for bearer shares issued on s no provision in law that prohibits transfer of bearer shares in other ways. Also, there are no provisions that require all bearer shares issued on paper to be deposited with the CSDC, or that prevent issuing new bearer shares on paper.

Criterion 24.12 Nominee shareholders and directors exist and are allowed, as a normal part of civil law contract law (freedom of contract and autonomy of will), as

confirmed by the SPC Provisions of the SPC on Several Issues Concerning the Application of Company Law, Arts. 24 28). The nominee shareholders and directors are to be presented to the outside world as if they are the actual or real shareholders or directors (principle of publicity) to ensure uninterrupted commercial transactions and protect bona fide third parties. There is no requirement to disclose nominee shareholders or directors, require them to be licensed and the status recorded, or other mechanism.

Criterion 24.13 A sufficient range of sanctions is available to the authorities, including but not limite

This Recommendation covers civil trusts: wealth, educational, and testamentary. Educational civil trusts aim to provide for funds for education, testamentary civil trusts aim to ensure that the will of a deceased is executed (as far as the distribution

to be managed by another person. This recommendation also covers foreign trusts that do business in China. This Recommendation does not cover business trusts (which are not a trust, but a financial product of trust companies, which are a type of FI) and charitable trusts (see R.8 for these).

Criterion 25.1 Even though the Trust Law creates the civil trust, there are no further requirements that require the identification of the settlor when establishing a civil trust and acting as a trustee, register the names of the settlor and beneficiary (note that this lack of further requirements may also impede on the ability to use the civil trust in practice, which is a factor taken into account in IO.5).

Criterion 25.2 There are no requirements regarding accurate recordkeeping for domestic civil trusts and/or for foreign legal arrangements operating in China.

Criterion 25.3 There are no requirements requiring trustees of domestic civil trusts and/or of foreign legal arrangements operating in China to disclose their status to an FI or DNFBP.

Criterion 25.4 There are no rules prohibiting trustees from disclosing their status. This is confirmed by cases provided by the authorities that showed foreign legal arrangements identified by banks as the beneficial owner.

Criterion 25.5 Law enforcement bodies and supervisors have the powers to obtain all of the information that FIs and other businesses hold, but there are no specific legal obligations that spell out that the three categories of information that this criterion requires are indeed available for civil trusts and foreign legal arrangements .

Criterion 25.6 There are no specific legal obligations that require information for civil trusts and foreign legal arrangements to be available for exchange with foreign partners, except if the information is with a bank and indeed can be legally exchanged with foreign partners.

Criterion 25.7 and 25.8 There are no rules for trustees of domestic civil trusts and/or of foreign legal arrangements operating in China regarding legal liability for failure to comply with obligations, and there are no sanctions available.

Weighting and Conclusion

The Trust Law creates civil trusts, but there is in general a lack of further requirements that could clarify the requirements of this Recommendation, although some of the criteria can be met in practice if banks have the relevant information on civil trusts and/or foreign legal arrangements in their CDD files.

[illegible]

In the Third Round MER, China was rated partially compliant with the former R.23, as the AML legislation in place did not apply to the securities and insurance sectors, and there were no AML/CFT supervisory programs.

Criterion 26.1 The PBC has been designated by the State Council as the competent authority for AML/CFT supervision of all FIs across China. Sectoral prudential regulators support the PBC (in the banking and insurance sectors by the CBIRC[79] and in the securities sector by the CSRC. These two Commissions are required to assist the PBC in its AML/CFT supervisory role; participate in the formulation of regulations governing the financial institutions they supervise and required to impose an obligation on such financial institutions to establish and improve an internal control system and perform other duties and functions as may be required by law (Arts. 9 and 36 of the AML Law of the PRC (Order of the President No. 56). The PBC is solely responsible for AML/CFT supervision in the non-bank financial sector, the Currency Exchange and the MVTS sector (Law of the PRC on the PBC, Art. 32(9); AML Law, Arts. 4 and 8; Provisions on AML Through Financial Institutions, Art. 3; Counter Terrorism Law, Art. 24). Payment institutions are not considered financial institutions in China, but have a designated AML supervisor, the PBC (Law of the People's Bank of China, Art. 32; AML Law, Arts. 8 and 34). The PBC is equally the designated supervisor for online lending institutions (Guiding Opinions of the People's Bank of China, the Ministry of Industry and Information Technology, the Ministry of Public Security, et al, on Promoting the Sound Development of Internet Finance (PBC Document No.[2015] 221)).

Criterion 26.2 In China, FIs are required to obtain permission from the competent financial authorities before conducting financial business. Requirements are as follows:

For Core Principles FIs: Banks: the Banking Supervision Law, Arts. 2 and 16; the Law on Commercial Banks, Arts. 11 and 12, and the Regulation of the PRC on the Administration of Foreign-Funded Banks, Art. 7; Securities Companies: the Securities Law, Art. 122; Insurance companies: the Insurance Law, Art. 67; Fund Companies: the Securities Investment Fund Law, Art. 13 and Measures for the Administration of Securities Investment Fund Management Companies, Arts. 2 and 14; Futures Companies: the Regulation on the Administration of Futures Trading, Art. 15 and Measures for the Supervision and Administration of Futures Companies, Art. 6.

For other FI: Banking Supervision Law of the People's Republic of China, Arts. 2 and 16; Trust Companies: Measures for the Administration of Trust Companies, Art. 7; Finance Companies: Measures for the Administration of Finance Companies of Enterprise Groups (2006 Amendment), Art. 6; Pilot Currency Brokerage Companies: Measures for the Administration of Pilot Currency Brokerage Companies, Art. 5; Financial Asset Management Companies: Regulation on Financial Asset Management Companies, Arts. 6 and 7; Financial Leasing Companies: Measures for the Administration of Financial Leasing Companies (2014), Art. 2; and Auto Finance Companies: Administrative Measures for Auto Finance Companies, Art. 2.

For payment institutions, including non-bank MVTS providers: Measures for the Administration of Payment Services of Non-Financial Institutions, Art. 3.

For currency exchange institutions: Administrative Measures for the Pilot Work of Franchised Individual Foreign Exchange Business, Art. 5.

79 The CBIRC was formed on 8 April 2018 by the amalgamation of the former CBRC and the former China Insurance Regulatory Commission (CIRC). However, in this chapter, references are to the former supervisors to be consistent with legal references.

Anti-

market orders and have no record of such violations for a minimum period of five years (Provisions on the Administration of the Qualifications for the Directors, Supervisors and Senior Executives of Insurance Companies, Order No.2 [2010] of the China Insurance Regulatory Commission).

Securities companies: The major shareholders (including actual shareholders) of a securities company are required, inter alia, to have no irregular or rule-breaking record during the most recent three years. Requirements similar in nature to the insurance sector apply to directors, supervisors and senior executives of securities companies (Securities Law, Arts. 124 and 129; Regulations on the Supervision and Administration of Securities Companies, Art. 10 â ‘•’ƒ•› ƒ™ ‘ˆ –Š‡ ‡‘’Ž‡ï• ‡’—„Ž‹ of China, Art. 146).

Fund companies: The major shareholders of a fund company are required, inter alia, to have no violations of law in the last three years. Persons with criminal records for corruption, bribery, malfeasance, property encroachment, or disruption of the socialist market economy are prohibited from serving as a director, supervisor, senior manager, or employee. The scope of background checks is limited to a few number of years. (Securities Investment Fund Law, Arts. 13 and 15). For directors the scope of background chec •™“9ë¹ C7i“C™Y•® ™Zã™R}Y–Æ [C™RTY– “Ø@ «Á 9•åà •2„ N°$ùBù‘DIÃ™T9•,U

that are applied to these FIs. Online lending institutions are not covered by PBC supervisory regulations, upon which the assessors place significant weight given its significance.

Criterion 26.5

c.26.5a The PBC requires each regulated institution to carry out the assessment of ML risk itself, with the PBC subsequently applying classifications and ratings on all FIs annually (Measures for the Administration of the Money Laundering Risk Assessment of Incorporated Financial Institutions (for Trial Implementation)). The assessment of classification and rating systems also factors in feedback and consultations with FIs; input on internal controls from sector financial regulators; reassessment by the PBC; and notification of reassessment results) and covers 20 criteria, including the improvement of AML policy and systems, mechanisms, technical support capability, personnel, customer identification, enhanced measures for higher-risk customers and business, recordkeeping, large-value and STRs, and reputation risk, training, internal audit and management.

These measures appear to be in effect for an indeterminate period as the authorities stated that no timeline was specified for when the regulations will be finalized. No measures are applicable to the online lending sector.

c.26.5b The classification and rating system described under c.26.5(a) is generally consistent with the ML/TF risks present in China. The authorities noted that the PBC has conducted sector risk assessments and imposes more frequent supervisory and inspection visits on higher risk sectors. For example, the banking sector is rated as higher risk than the securities and insurance sectors generally. No measures are applicable to the online lending sector.

c.26.5c The risk classification and grading system considers the characteristics of financial institutions or groups (see c.26.5a). Financial institutions are required to provide sufficient supporting materials on the conclusions of self-assessment. The most significant financial institutions in China are supervised directly by PBC HO; this group includes the largest banking and insurance groups in China. No measures are applicable to the online lending sector.

Based on the foregoing, the PBC conducts AML/CFT onsite and offsite supervisory measures accordingly. Statistics submitted to the assessors confirmed that the frequency and intensity of supervisory measures on higher-risk financial institutions is higher than those at lower-risk institutions. (Measures for the Administration of Anti-Money Laundering Categorized Ratings of Incorporated Financial Institutions (for Trial Implementation), Art. 12).

The principle shortcoming is that the measures are not applied in the online lending sector, upon which the assessors place significant weight given its significance.

Criterion 26.6 The PBC institutional (or group) AML/CFT assessment is conducted annually based on the process noted above. When there are major AML/CFT risk events in the FIs or groups, their rating is reassessed, which can result in more frequent or intense scrutiny (Measures for the Administration of Anti-Money Laundering Categorized Ratings of Incorporated Financial Institutions (for Trial Implementation), Chapter 1). Authorities stated that a similar approach is used in the payment institutions sector. No measures are applicable to the online lending sector.

Weighting and Conclusion

The online lending sector is subject to limited obligations set out in (Guiding Opinions of the People's Bank of China, the Ministry of Industry and Information Technology, the Ministry of Public Security, et al, on Promoting the Sound Development of Internet Finance (PBC Document No. [2015] 221) but is not supervised for AML/CFT requirements. The assessors have given a significant weighting to this omission on the basis of the extent of the sector and the conclusion in the NRA which is that as AML control measures do not reduce the inherent risk, the residual vulnerability of the online lending sector is high. There are shortcomings in the market entry requirements mostly relating to the limited mandatory periods for criminal record searching.

Criterion 27.4 The PBC and the sectorial financial supervisors are authorised to impose a range of sanctions on FIs and payment institutions for failure to comply with the AML/CFT requirements as set forth in R.35 including: warning, ordering to correct, fine, confiscation of illegal proceeds, ordering of suspension or revoking of the qualification to hold a post, disciplinary sanction, prohibiting him/her from engaging in financial sectors, etc.

Relevant laws that grant the supervisors power to impose sanctions on FIs and payment institutions unless noted differently:

- Law of the People's Republic of China on the People's Bank of China, Art. 46;
- AML Law, Arts. 31 and 32;
- Counter Terrorism Law, Art. 83;
- Banking Supervision Law, Art. 37; covers banks;
- Measures for the Administration of Payment Services of Non-Financial Institutions (Order of the People's Bank of China No. [2010] 2), Art. 44; covers payment institutions;
- Measures for the Anti-Money Laundering Work in the Securities and Futures Sectors, Art. 17; covers securities and futures entities;
- Measures for the Administration of Anti-Money Laundering Work in the Insurance Sector, Art. 36; covers insurance companies;
- Administrative Measures for the Freezing of Assets Relating to Terrorist Activities, Art. 19; and
- There are no measures covering online lending institutions.

Weighting and Conclusion

Sanctions are not in line with the standards set out in R.35 (see TC Annex R.35).

[illegible]

In the Third Round MER, China was rated non-compliant with former R.24, mostly due to the fact that DNFBPs were not covered by AML/CFT obligations, and the penalty structure for trust companies was deficient.

Art. 35 of the AML Law provides that the specific measures for supervision and administration on DNFBPs shall be formulated by the PBC (the administrative department of AML of the State Council) in collaboration with the relevant departments of the State Council.

During the onsite visit the PBC purported to issue Notice of the General Office of the [illegible] China on Strengthening the Anti-Money Laundering Supervision Work on Designated Non-Financial Businesses and Professions, 2018 which purported to enter into force on July 26, 2018. This Notice purported to designate the DNFBPs as follows:

- : when they are involved in transactions for their clients concerning the buying and selling of real estate;
- , including institutions providing a place to dealers for the sale of precious metals and precious stones: when they engage in or provide services for spot trading of precious metals and precious stones;
- , when they prepare for or carry out transactions for their clients concerning the following activities: buying and selling of real estate; managing of client money, securities or other assets; management of bank or securities accounts; organisation of contributions for the creation, operation of companies; creation, operation or management of legal persons or arrangements, and buying and selling of business entities; and
- , when they prepare for or carry out transactions for a client concerning the following activities: providing professional services for the creation, operation and management of a company; acting as (or arranging for another person to act as) a director of a company, a partner of a company, or act as a shareholder of a company; providing a registered address, business address or correspondence address and so on.

The assessment of regulation and supervision requirements for trust companies is made under R.26 and R.27, since they are FIs in China and their designated AML/CFT supervisor is the PBC, supported by the CBRC. However, in the context of the FATF standards, trust companies are DNFBPs (trust service providers) covered by AML/CFT obligations.

Notwithstanding the foregoing, for the reasons further stated under R.22, the assessors do not believe that the above designation was completed as required under the AML Law, and accordingly DNFBPs (except for DPMs and trust companies) are not subject to AML/CFT obligations.

Criterion 28.1 (Not applicable) It is prohibited to operate a casino in China. Gathering a crowd for gambling, making a living on gambling, or operating a casino constitute crimes (Criminal Law, Art. 303).

Criterion 28.2 Art. 35 of the AML Law provides that the specific measures for supervision and administration of DNFBPs shall be formulated by the PBC (the administrative department of AML of the State Council) in collaboration with the relevant departments of the State Council. The purported designation referred to above does not specify which AML/CFT measures will apply to DNFBPs and therefore it appears that all measures in the AML Law would apply to these DNFBPs if the designation was effective. However, the PBC has not implemented any measures for supervision and administration of DNFBPs except for trust companies and DPMs.

Criterion 28.3 The purported designation of the DNFBPs subject to the AML Law (as set out above) took place during the on-site visit, and thus there were no systems in place for monitoring the DNFBPs (apart from trust companies and DPMs) for compliance with AML/CFT requirements.

Criterion 28.4

- Art. 35 of the AML Law provides that the specific measures for supervision and administration of DNFBPs shall be formulated by the PBC (the administrative department of AML of the State Council) in collaboration with the relevant departments of the State Council (sector supervisors). However, as noted above the PBC has not properly formulated such measures;
- Insufficient information has been provided on how the authorities prevent criminals or their associates from being professionally accredited or holding ownership or a management interest in some DNFBP sectors as (de from trust companies and DPMs); and
- It is not clear which sanctions are available for the designated DNFBPs (aside from trust companies).

Criterion 28.5 As of the date of the on site visit there was no supervision in the DNFBP sector (aside from trust companies) by the PBC as the sector was only designated on July 26, 2018.

Weighting and Conclusion

Only DPMs and trust companies are subject to any measures, applied by the sector SRO (DPMs) and the PBC (trust companies) respectively. The assessors have given significant weighting to the many DNFBP sectors not covered by AML/CFT preventive measures, particularly the real estate sector.

[illegible]

In the Third Round MER, China was rated largely compliant with these requirements (para. 187 239). The main technical deficiency was that the FIU did not have (timely)

effectiveness of the FIU, which was not assessed as part of technical compliance under the 2013 Methodology.
been significantly strengthened in this area by imposing new requirements which

to disseminate information upon request and request additional information from reporting entities.

Criterion 29.1 China established a decentralised FIU within the PBC (PBC Law, Art. 4(10)) that consists of the following components, which function largely independently from each other and with limited systematic coordination between each other.[80] The assessment team recognises that a country has the choice to implement a decentralised FIU approach and does not question nor criticize the fact that China has chosen this approach. However, the assessment team has serious concerns regarding the implementation of this decentralised approach in China, which limits its ability to act as a national centre for receipt and analysis of suspicious

80 The AML Law

transaction reports and other information relevant to money laundering, associated predicate offences and terrorist financing; and for the dissemination of the results of that analysis.

- CAMLMAC;
- AMLB; and
- AML Units within each of the 36 provincial PBC branches (hereafter referred to as the PBC provincial branches).

CAMLMAC is established at the central level and has primarily responsibility for the receipt and analysis of ordinary STRs (i.e., transactions related to criminal activities such as ML, TF, and predicate offences – STRs) and large-value transaction reports (LVTRs). CAMLMAC also receives the information contained in all key STRs directly and simultaneously reported to the 36 provincial PBC branches (see analysis of R.20 and below). It reports the results of its analysis to central LEAs or other competent authorities or passes the information on to the AMLB or a PBC provincial branch for an administrative investigation (AML Law[81] Arts. 8 and 10). CAMLMAC and the AMLB conduct joint analysis of complex cases identified and transferred to them by the PBC provincial branches.

While the AMLB is primarily a policy-driven unit, it also has the power to conduct administrative investigations of STRs identified by CAMLMAC and takes independent decisions in terms of dissemination to central or local LEAs and other competent authorities. In addition, the AMLB coordinates and steers administrative investigations with cross-regional aspects conducted by PBC provincial branches (AML Law, Arts. 8, 23 – 26). As mentioned above, the AMLB and CAMLMAC conduct joint analysis of complex cases.

The PBC provincial branches are the primary recipient of key STRs[82] identified by local financial institutions, and whistle-blower reports. In addition to the analysis/investigation of these types of reports, the provincial branches are also responsible for conducting administrative investigations based on suspicious activity

branches (AML Law, Arts. 8, 23 – 26). They disseminate the results of their analysis and administrative investigations to local LEAs without direct access to information collected, analysed and disseminated by the other FIU components at central or local level, nor systematic coordination with any of these other FIU components. Each of the PBC branches registers the information collected during its analytical/investigative process and the subsequent disseminations in a stand-alone database, which is not accessible outside the PBC branch itself. The PBC provincial

81 Art. 2 of AML Law – refers to an act of adopting the relevant measures according to the provisions of the Law to prevent any money-laundering activity with the purpose of concealing or disguising the sources and nature of criminal proceeds generated from any concealing drugs crime, organizational crime of any gangland, terrorist crime, crime of smuggling, crime of corruption or bribery, crime of disrupting the financial management order, crime of financial fraud, etc. Art. 36 specifically extends the scope of the AML Law.

82 Key STRs are defined as follows: (i) The transaction is evidently suspected of ML, TF, or any other criminal activity. (ii) The transaction seriously compromises national security or affects social stability. (iii) Any other serious circumstance or emergency.

branches provide the details of these disseminations to CAMLMAC to ensure that the information disseminated is on record.

CAMLMAC thus centrally registers the details of all types of reports (STRs, key STRs, and LVTRs) received by both CAMLMAC itself and the 36 provincial branches, as well as the details on information disseminated by the three FIU components. However, provincial branches is limited to transactions executed in their province but branches can obtain other information from CAMLMAC upon request.

Criterion 29.2

C.29.2a CAMLMAC receives all STRs and the information in all key STRs, which FIs directly and simultaneously report to the PBC provincial branches (Measures for the Administration of Financial Institutions' Reporting of Large-Value Transactions and Suspicious Transactions, Arts. 11 and 17). CAMLMAC thus centralises the receipt of all types of reports. This is important because, as mentioned in c.29.1, each PBC provincial branch operates a stand-alone database, which is not accessible by CAMLMAC, the AMLB or any other PBC branch.

C.29.2b CAMLMAC also receives:

- LVTRs, including large-value cash transactions, large-value transfer transactions, and large-value cross-border transactions[83] (AML Law, Art. 10 and

reporting entities more broadly, then it has to transfer the case for an administrative investigation to the AMLB or one of the provincial branches.

The AMLB and the PBC provincial branches have the power to obtain all relevant information, documents and materials from any reporting entity when conducting an administrative investigation (AML Law, Chapter IV, Arts. 23–26, and Notice of the People's Bank of China on Issuing the Detailed Rules for Anti-Money Laundering Investigations, Art. 6).

c.29.3(b) – The FIU components at all levels have the power to access, either directly or upon request, a wide range of financial, administrative, and law enforcement information, as well as information from public sources (Art. 11 of the AML Law).

Criterion 29.4

c.29.4(a) – CAMLMAC conducts operational analysis of STRs and LVTRs and based on requests received from LEAs (Regulation on the Main Responsibilities, Internal Departments and Staffing of CAMLMAC, PBC Document [2010] No. 16). It also has full access to the information contained in key STRs directly and simultaneously reported to the PBC provincial branches to support its analysis of STRs and LVTRs. In addition, as set out in c.29.1 above, CAMLMAC also conducts operational analysis jointly with the AMLB of complex cases transferred by the PBC provincial branches. Moreover, the administrative investigations by the AMLB and the PBC provincial branches do also qualify as FIU operational analysis (AML Law, Art. 8 and 10, and the Regulation on the Main Responsibilities, Internal Departments and Staffing of AMLB, PBC Document [2010] No. 8, and similar documents for each individual PBC branch).

The PBC provincial branches keep the information collected in the course of their initial operational analysis/administrative investigation and the results of this analysis/investigation in a stand-alone database, which CAMLMAC, the AMLB or any other provincial branch cannot access. In addition, as mentioned above in c.29.1, the provincial branches have
database, namely to details of transactions executed in their province. Therefore, the three FIU components do not have access to all information available and obtainable by the FIU for use in operational analysis to follow the trail of particular activities or transactions, and to determine links between those targets and possible proceeds of crime, money laundering, predicate offences and terrorist financing, as required by c.29.4(a).

c.29.4(b) – The three FIU components conduct strategic analysis to guide financial institutions in the identification of STRs and key STRs, and to provide policy guidance and steering to LEAs and other competent authorities. However, the same limitation as identified in c.29.4(a) with regard to the use of available and obtainable information applies to c.29.4(b).

Criterion 29.5 – As mentioned above with regard to c.29.1, all three FIU components independently disseminate the results of their analysis/investigation to central or local LEAs, both spontaneously and upon request (AML Law, Art. 4 and 13). The CAMLMAC, AMLB, and PBC provincial branches have established cooperation mechanisms with LEAs and other competent authorities as the basis for the dissemination of data. The CAMLMAC, AMLB and the PBC provincial branches disseminate the results of their analysis by using secure and protected channels.

Criterion 30.3
State Security Agencies, and Customs have powers to identify, trace, freeze, and seize suspected POC or property that is, or may become, subject to confiscation (CPL, Arts. 100, 139, 142, 280; see also c.4.2 above).

Criterion 30.4 R.30 applies to all relevant authorities responsible for investigating predicate offences.

Criterion 30.5
refer ML aspects to the public security agencies for investigation.

Weighting and Conclusion

[redacted]

In the Third Round MER, China was rated compliant with these requirements. The new R.31 was expanded and now requires countries to have, among other provisions, mechanisms for determining, in a timely manner, whether natural or legal persons hold or manage accounts.

Criterion 31.1 LEAs and other competent authorities are authorised to use a wide range of powers when conducting investigations of ML, TF, and predicate offences. These powers include:

- the production of records held by financial institutions, DNFBPs, and other natural, or legal persons (CPL, Art. 135);
- the search of persons, articles, houses, and other premises where suspects or criminal evidence may be hidden (CPL, Art. 134);
- taking witness statements (CPL, Arts. 52 and 122); and
- the seizure and compulsory acquisition of articles and other materials relevant to the crimes (CPL, Arts. 139, and 142; and Provisions of Public Security Agency (PPSA) handling procedures of criminal cases).

These powers can be exercised, subject to the LEAs obtaining a search warrant or other relevant authorisation. These powers can also be used together with freezing and confiscation actions. Likewise, the customs and tax authorities also have powers of inquiry, detention, freezing, search, and questioning when investigating cases under their jurisdiction (Customs Law, Arts. 2, 4, 6(5), and 61 (I)(ii); and Law of the [redacted] Art. 57). The evidence acquired (including any frozen funds or detained articles) can be used in any subsequent prosecution and enforcement procedures.

Criterion 31.2 LEAs are entitled to adopt special investigation techniques for which the legal basis is included in the CPL and the PPSA handling procedures. Such techniques include:

- undercover operations (CPL, Art. 151 and PPSA handling procedures, Art. 262);

- monitoring, inspection, and verification of electronic communication devices (PPSA handling procedures, Art. 255);
- accessing computer systems (PPSA handling procedures, Art. 112); and
- controlled delivery and controlled payments (CPL, Art. 151, and PPSA handling procedures, Art. 263).

These powers can be used in the context of ML and TF investigations, subject to approval formalities to ensure that relevant requirements for use of these techniques, as set out in Arts. 148 152 of the CPL and Arts. 254 264 of the PPSA, are respected. The evidence obtained can be used in court.

Criterion 31.3 LEAs have the power and several (online) mechanisms in place through which they are able to identify whether natural or legal persons hold or control accounts. They also have a process in place to identify assets without prior notification to the owner. These powers are set out in the following legal documents: for Public Security Agencies: CPL, Art. 135 and PPSA handling procedures, Arts. 231 CPL, Art. 142 and Rules on Criminal Procedure of the People's Procuratorates, Arts. 141 and 142; for State Security Authorities: CPL, Art. 4; and for Customs: Customs Law, Art. 6(5) and Regulation on Customs Inspection, Arts. 10 and 14).

Criterion 31.4 As set out with regard to c.29.5 above, the three FIU components can cooperate with LEAs and provide them assistance with their investigations into ML, predicate offences, and TF activities and disseminate upon request. (AML Law, Art. 4, and Regulation on the Main Responsibilities, Internal Departments and Staffing of the CAMLMAC, AMLB, and local branches, PBC Documents 16, 8, and others, respectively).

Weighting and Conclusion

[illegible]

In the Third Round, China was rated partially compliant with these requirements (para. 271 299) because the reporting system in place exclusively focused on cash and BNI was not included. In addition, reports on cash declarations/seizures were not being provided to the FIU and were not being used to identify and target money launderers and terrorist financiers. The new Recommendation (R.32) contains new requirements regarding the declaration system and the safeguards in place to ensure the secured use of information collected.

Criterion 32.1 China implemented a declaration system for incoming and outgoing cross-border transportation of both national and foreign currency at all ports of entry to/departure from China, including airports, seaports, and rail and road crossings (Announcement of the General Administration of Customs: Notice of Implementation of New Declaration Formalities for Passengers Entering and Leaving the Country at All Open Ports, Art. III.5).

Travelers should declare to Customs all physical inward and outward transportations of national currency in cash above the prescribed threshold of RMB20 000 (USD2 935). While drafts, checks, and promissory notes should record information

on the beneficiaries and a lack of such information results in these negotiable instruments being invalid (Negotiable Instruments Law, Arts. 22, 75, 84, and 86), checks. The declaration China has a prohibition on the transportation of national currency through mail and a prior authorisation applies to transportation of national currency through cargo (Decree 43 of the General † • ‹ • ‹ • – ” ƒ – ‹ ‘ • ‘ ^ — • – ‘ • • ‘ ^ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ‡ 4 and Ž 5 of the ^ Š ‹ • ƒ á ƒ • † Control Procedures of China on Carrying the State Currency into or Out of the Country).

For foreign currency any amounts over USD 5 000 (or any equivalent foreign currency) in cash carried into or out of China is subject to an application for a Permit for Carrying Foreign Exchanges into and out of the country. In addition to carrying the corresponding certification document, travellers should also declare the transportation of the foreign currency to Customs. (Notice of the State Administration of Foreign Exchange and the General Administration of Customs on Issuing the Interim Measures for the Administration of Carrying Foreign Currency Cash for Persons Entering or Exiting the Territory, and Interim Measures for the Administration of Carrying Foreign Currency Cash for Persons Entering or Exiting the Territory, Art. 3). Transportation of foreign currency in cash through mail and cargo is also subject to prior authorisation (Decree 43 of the General Administration of Customs of the ‘ P Ž ‡ ï • Republic of China). The relevant provisions are silent with regard to foreign BNI and the declaration obligation does therefore not extend to foreign BNI.

Chinese authorities provide that there is no BNI operation in the country and customs and financial institutions have not identified any BNI over the last three years.

compliance with each of the individual criteria below.

Criterion 32.2 China has a written declaration system in place for all travellers carrying national currency in cash above RMB 20 000 (USD 2 935) or foreign currency in cash above USD 5 000. The declaration obligation does not extend to

Criterion 32.3 China has not implemented a disclosure system for the purposes of R.32.

Criterion 32.4 Customs has the authority to request and obtain further information from the carrier with regard to the origin and the intended use of the cash upon discovery of a false declaration or a failure to declare national and foreign currency in cash. (Customs Law, Arts. 2, 6, and 12; and Regulation on the Implementation of Customs Administrative Punishments, Arts. 33, 34, 43).

Criterion 32.5 There exists a wide range of proportionate and dissuasive sanctions for making a false declaration or failing to declare. Almost all of the relevant sanctions include the ability to freeze, seize, and confiscate the cash involved.

A false declaration is a violation of the Customs Law, Art. 82(1) and of the Regulation on the Implementation of Customs Administrative Punishments, Art. 7(2) and is subject to warnings, administrative fines or criminal penalties (Customs Law, Art. 82 and Regulation on the Implementation of Customs Administrative Punishments, Art. 9(2)). A fine applies to a false declaration or a failure to declare by a legal person or other entity. In addition, Customs can issue a warning to the person in charge or the directly

responsible personnel, but also has the power to sanction the individual with a fine up to RMB50 000 (approx. USD7 338) (Regulation on the Implementation of Customs Administrative Punishment, Art. 32).

A case of failure to declare qualifies as [currency] smuggling. In such instances, the Customs has the power to confiscate the smuggled currency and proceeds from any illegal activities and charge a fine (Customs Law Art. 82, and Regulation of the People's Republic of China on the Implementation of Customs Administrative Punishment, Art. 9 (2)). Moreover, in addition to a fine, criminal sanctions, including imprisonment, apply to individuals. (Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Trial of Criminal Cases of Smuggling, Art. 2).

Other cases of failure to declare, but without the intention to smuggle currency in or out of the country, are subject to a warning, and a fine up to 20% of the amount concerned. (Customs Law, Art. 85 86, and Regulation on the Implementation of Customs Administrative Punishment, Art. 19(3) (4)).

Criterion 32.6 In 2017, authorities started working on setting up a system for Customs to notify CAMLMAC of information on cross-border transportation violation cases but the system is only in its very early implementation stages. While Customs periodically informs the FIU of excessive undeclared amounts of cash, the information made available does not specifically focus on ML or TF suspicions.

Criterion 32.7 China makes use of both its Anti-Money Laundering Coordination Mechanism and its Anti-Smuggling Coordination Mechanism to coordinate on issues related to the implementation of R.32. Cooperation and coordination between Customs and public security agencies (e.g. departments of immigration and emigration administration and departments of frontier inspection) coordinate and cooperate, in particular at border ports (Customs Law, Arts. 4 and 5; and Exit and Entry Administration Law, Art. 6). However, as mentioned in c.32.6 above, the information sharing mechanism with the FIU is only in its very early implementation stages.

Criterion 32.8 Customs have the power to inspect particular, suspicious, or random targets; check and examine cross-border vehicles, goods, and articles, and detain for up to 48 hours items, goods, and articles in violation of relevant laws and administrative regulations, including the regulations on the control of the cross-border transportation of cash. Customs also have the power to seize undeclared cash or impose punishments on the identified illegal transportation of cash that exceeds the prescribed thresholds, as set out above with regard to c.32.5 (Customs Law, Art. 6; and Regulation on the Implementation of Customs Administrative Punishment, Art. 38).

Criterion 32.9 As mentioned above with regard to c.32.7, the information made available to the FIU only covers declaration violation cases of excessive amounts, including false declarations, but does not specifically extend to suspicions of ML and TF. The FIU has the power to exchange this information with its foreign counterparts. The same information is also available for exchange with foreign customs authorities based on MLA agreements, MOUs, and international conventions.

Criterion 32.10 China has strict safeguards in place to ensure proper use of the information collected through the declaration system (General Provisions of the Civil Law of the PRC, Art.111 and CFT Law, Art.48). The cross-border declaration system

does not appear to restrict trade payments between countries nor the freedom of capital movements (Customs Law Arts. 71, 72, and 75).

Criterion 32.11 The wide range of sanctions mentioned above in c.32.5, including seizure and confiscation, equally apply to persons who carry out a physical cross-border transportation of currency that is related to ML and TF. In addition, in such cases, persons also qualify for criminal sentences of ML and TF, as set out in R.3 above.

Weighting and Conclusion

The declaration requirement does not extend to BNI but this deficiency carries less weight because China prohibits most types of domestic BNI. The relevant information that the FIU receives from the customs authorities only covers declaration violation cases of excessive amounts and does not specifically extend to false declaration or suspicions of ML and TF.

[illegible]

In its Third Round MER, China was rated largely compliant with these requirements. The main technical deficiencies were that no statistics were kept concerning the number of cross-border transportations of currency and bearer negotiable instruments, and the time taken to respond to extradition requests. In addition, there were no statistics available on the number of freezing, seizing or confiscation actions, or the amount of assets involved.

FIU

[illegible]

c.33.1a CAMLMAC centrally collects and maintains the statistics on the receipt of [illegible]-branches and disseminations to LEAs, by all three FIU components, both spontaneously and upon request. CAMLMAC can produce these statistics in real-time using its IT system.

c.33.1b [illegible] ML/TF investigations, prosecutions, and convictions. The PBC keeps statistics on administrative investigations stemming from STRs.

[illegible] relating to ML investigations, TF investigations, and ML/TF prosecutions and convictions respectively. China qualified statistics provided as samples as not all judgments are publicly available and therefore statistics provide were not comprehensive.

c.33.1c The Ministry of Public Security, the Ministry of State Security, the General [illegible] deposits however it is unclear whether comprehensive statistics are kept on funds frozen. While China has issued an Opinion on Further Regulating the Disposition of

Property Related to Criminal Proceedings which indicates that investigative authorities should input relevant case related property information into a centrally managed system, this system is not yet fully functional.

judgements.

All illegally gained property, regardless of the crime, is turned over to the State Treasury which is supervised by the Ministry of Finance. The Ministry of Finance is responsible for maintaining statistics on confiscations from the different authorities.

c.33.1d

statistics on extraditions and MLA requests sent and received. The Ministry of Public Security maintains statistics on cross border police to police cooperation, and the PBC maintains statistics related to financial intelligence sharing with foreign FIUs.

Weighting and Conclusion

While statistics are largely kept on the four main areas covered by R.33, China was not always able to breakdown the statistics into meaningful sub-components and at times needed to rely on samples.

[illegible] - [illegible]

In its Third Round MER, China was rated largely compliant with these requirements. The main deficiency was that no guidance had been issued in relation to what were, at the time, new obligations under the enacted AML Law (2006) and connected regulations.

Criterion 34.1

Supervisory Guidance

The PBC, CBRC, CSRC, and CIRC have developed a series of published Guidelines and Notices to guide the FIs and payment institutions in performing AML/CFT work. The guidelines include:

- The PBC and the sector financial regulators instruct financial industry associations to establish guidance for their industry (

The PBC has published 33 Money Laundering Risk Warnings to the end of 2017, and PBC branches also issued some Money Laundering Risk Warnings for guiding the financial institutions to focus on high-risk areas of ML/TF.

financial regulators and FIs about the external threats of ML/TF and the key issues identified during supervision. The PBC shares with the CBRC, CSRC, and CIRC information about the AML supervision information of FIs, which promote the FIs to perform their duties in compliance with relevant laws and regulations.

For AML enquiries that are raised by the FIs, the PBC conducts research and issues professional interpretations.

No guidance applies to online lending institutions.

Trust companies are considered as FIs in China and are subject to guidance and feedback as described above. However, in the context of the FATF standards, trust companies are DNFBPs (trust service providers). Guidance specifically directed to the provision of trustee services does not appear to be issued. Little or no guidance was issued to other categories of DNFBPs.

FIU Guidance and Feedback

CAMLMAC provides reporting institutions with the various formats for the reporting of suspicious and large value transactions. Art. 28 of Measures for the Administration of Financial Institutions' Reporting of Large-Value Transactions and Suspicious Transactions provides that if reports submitted by a FI are incomplete or erroneous, CAMLMAC may send a notice of supplementation and correction to the FI. According

system automatically and systematically reviews the completeness of the reports submitted. Such feedback involves an acknowledgement of receipt and automatic verification of the completeness of LVTRs and STRs submitted by reporting institutions. In addition, CAMLMAC provides annual feedback on the quality of the STRs and LVTRs to reporting institutions. This comprises both written and face-to-face feedback.

Weighting and Conclusion

DNFBPs (aside from trust companies and DPMS) are not subject to the AML Law and hence related guidance is not applicable.

[illegible] - Sanctions

In its Third Round MER, China was rated partially compliant on the former R.17. The effectiveness of penalties provided in the AML Law for major deficiencies was relatively low. The penalty system focused excessively on minor deficiencies and was ineffective in dealing with structural weaknesses.

Criterion 35.1

Where an FI or a DNFBP fails to immediately freeze the funds or other assets of any designated terrorist organisation

or terrorist, the public security agency shall impose a fine of not less than RMB 200 000 (approx. USD 29 352), but not more than RMB 500 000 (approx. USD 73 380) on the institution, and impose a fine of not more than RMB 100 000 (approx. USD 14 676) on its directly responsible directors, senior executives, and other directly liable persons. If the circumstances are serious, these fines may be increased to not less than RMB 500 000 (approx. USD 73 380) on the institution, and not less than RMB 100 000 (approx. USD 14 676) but not more than RMB 500 000 (approx. USD 73 380) on its directly responsible directors, senior executives, and other directly liable persons; may revoke its business license and order it to cease operations; and may detain such natural persons for not less than 5 days, but not more than 15 days (Counter Terrorism Law of the Peoples Republic of China, Order of the President No. 36, Arts. 83 and 93). Coverage of DNFBPs (apart from trust companies) only took effect on July 26, 2018 when such DNFBPs were designated under the AML Law by PBC.

If the circumstances are serious, the competent department can order the FI to cease doing business (Art. 93 of the Counter Terrorism Law). The FI may also be subject to sanctions imposed by the PBC (Art. 19 of Administrative Measures for the F8 (mainland) epublic of

and record keeping; additional measures for specific customers and activities; reliance, controls and financial groups; reporting of suspicious transactions): When an FI fails to establish a prescribed internal control system of AML, or fails to establish an AML institution or an internal department on AML, or fails to conduct AML training for employees, it shall be liable to receive an order to correct the deficiency within a time limit. If the deficiency is serious, the PBC may order the sectorial supervisor to apply a disciplinary sanction to the chairperson, senior management or any other person as well (Art.31 of AML Law). These penalties appear to apply to failures to comply with AML Law, Art. 15 (internal control systems and specialized AML unit), and 22 (training). For more serious violations, the financial penalties noted above under Art. 32 of the AML Law will apply.

Where an FI fails to comply with the AML Law in the following circumstances (i) performing CDD (Art. 16, 17, 18, 21); (ii) keeping records (Art. 19, 21); (iii) reporting large-value or suspicious transactions (Art. 20, 21); (iv) dealing with a client without completing identify verification or establishing anonymous or pseudonymous accounts; (v) violating confidentiality provisions; (vi) retarding AML examinations or investigations; and (vii) refusing to provide investigations material or provides false material on purpose.; the PBC can order the institution to correct the breach. Where the breach is serious the institution can be fined RMB 20 000 50 000 (approx. USD 2 935 7 338, and a natural person can be fined RMB 10 000 50 000 (approx. USD 1 467 7 338). Where the breach leads to ML, a fine of RMB 500 000 up to RMB 5 million (approx. USD 73 380 733 804 shall be imposed upon the FI and a fine of RMB 50 000 up to RMB 500 000 (approx. USD 7 338 73 380) shall be imposed upon its directly liable director, senior management, or any other person. In the case of particularly serious circumstances, the PBC may advise the sectorial regulator to order the FI to suspend its business for rectification or to revoke its business license. However, given that the highest sanctions only apply when ML occurs, their availability is confined to limited circumstances, which affects their effectiveness.

As to the directly liable director, senior management, or any other person of an FI, the PBC may advise the relevant financial regulatory body to order the FI to give a disciplinary sanction thereto or revoke his/her qualification to hold a post and prohibit him/her from engaging in any financial work (Art. 32 of the AML Law).

Art. 49 of the Measures for the Administration of Anti-Money Laundering and Combatting the Financing of Terrorism for Payment Institutions PBC Document 2012 (54) provides that where payment institutions violate AML/CFT requirements, they can be sanctioned in accordance with the provisions of Arts. 31 and 32 of the AML Law.

As of the date of the onsite visit, the foregoing measures apply to designated DNFBPs (apart from trust companies) (Art.

Entities and individuals who are subject to the above penalties and who have

Recommendation 36 – International instruments

In its Third Round MER of 2007, China was rated partially compliant with requirements for former R.35 and SR.I. The main deficiencies were that criminalization of ML, the seizure/confiscation regime, and preventative measures were not fully in line with the Vienna, Palermo, and TF Conventions. There was also a deficiency of inadequate implementation of UNSCR 1267 and 1373, but that is no longer assessed under this Recommendation.

Criterion 36.1 China is a party to all four conventions. China ratified the Vienna Convention on October 25, 1989, the Palermo Convention on September 23, 2003, the Merida Convention on January 13, 2006, and the Terrorist Financing Convention on April 19, 2006.

Criterion 36.2 China has substantially implemented the Vienna, Palermo, Merida, and TF Conventions. There are some aspects that might impact the implementation of the conventions: for example, equivalent value confiscation is reached through mandatory confiscation court ruling (see for more detail R.4), and self-laundering is not criminalised (see for more detail R.3). Not all of the terrorist acts referred to in the conventions and protocols listed in the Terrorist Financing Convention are criminalis
and maritime sectors, protected persons, nuclear materials (see for more detail R.5). Some crimes are formulated too generally in the Criminal Law, which might present difficulties in the prosecution process.

Weighting and Conclusion

China has ratified and substantially implemented the international conventions required by R.36, although not all offences set in these conventions are offences under the Chinese law.

Recommendation 37 – Mutual legal assistance

In its Third Round MER, China was rated compliant (R.36) and largely compliant (SR.V) with these requirements. The main deficiency was a partial coverage of the TF offence in Art. 120bis CL (sole collection of funds not criminalized) which constituted an impeding element when applying the dual criminality principle in relation to a foreign MLA request

Criterion 37.1 The Criminal Procedure Law, AML Law, and other relevant laws of China set a legal basis for providing MLA (Art. 17 of the Criminal Procedure Law). China provides MLA, in AML/CFT investigations including, on the basis of bilateral MLA treaties and international conventions that China is a party to, or under the principle of reciprocity (Art.17, CPL; Art. 29, AML Law; Art. 68, Counter Terrorism Law). China can provide a wide range of legal assistance to foreign countries in investigations, prosecutions, and related proceedings involving ML or related predicate offences and TF although due to the complexity of the procedures it is not rapid as a rule.

Criterion 37.2 There are two principal channels of communication for MLA in China depending on what legal basis the MLA is to be provided.

Under general circumstances, the MoJ of China is the central authority for international conventions and bilateral treaties on MLA. The MoJ will pass the requests on to the authority competent to take the requested actions according to Chinese laws. Besides, the MoJ is responsible for following up the implementation. Additionally, some treaties or ratification notes for conventions have designated the MPS (for example, for the Palermo Convention) or the SPP (for example, for the Merida Convention) as central authorities, which are in charge of receiving, investigating, transmitting, and coordinating criminal legal assistance cases.

Outside the context of a convention or an agreement, the MFA is the correspondent in China. It reviews the request, forwards it to the appropriate law enforcement authority, and channels the reply. The MLA is granted in such a case on the condition of a commitment of reciprocity to China.

The SPC, the SPP, the MPS, and the MFA have procedures for criminal legal assistance to ensure the timely handling of requests for criminal legal assistance (Interpretations of the Supreme People's Court on the Application of the Criminal Procedure Law of the People's Republic of China, Chapter 18; Rules of Criminal Procedure of the People's Procuratorate, Chapter 16; Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies, Chapter 13).

There are specific provisions for the process related to the execution of foreign requests, but there are no requirements for prioritizing them. The MoJ, the SPP, the MPS, the MFA, and other authorities have internal case management systems to supervise the procedures of processing the cases involving legal assistance but not prioritization.

Criterion 37.3 In China the legal conditions for MLA are international treaties that have been concluded or acceded to by China or the principle of reciprocity. Requests that do not conform to the provisions of the treaties or the relevant laws are not enforced by China. In addition, damaging the sovereignty, safety, and public interests of the country or violation of the Chinese laws are other reasons for rejection of MLA (CPL, Art. 17). The latter is in line with the principles and traditions of international mutual legal assistance.

Criterion 37.4 Based on the legal framework, China would not refuse a request for legal assistance due to (i) fiscal issues or (ii) confidentiality issues, except in cases covered under c.37.3.

Criterion 37.5 The Secrecy Law of China stipulates that the secrets in diplomatic and foreign affairs, the secrets bearing the obligations of confidentiality and the secrets related to the criminal offences are state secrets protected by law. All state agencies, armed forces, political parties, public organisations, enterprises, and citizens have the duty to protect state secrets (Secrecy Law, Arts. 3, 9). The Criminal Procedure Law sets that evidence involving any state secrets, commercial secrets, or personal privacy shall be kept confidential (Art. 52).

Criterion 37.6 China uses dual criminality as a condition for providing MLA. (Criminal Law, Art. 7 9). In certain situations, China can negotiate with a foreign party

For example, the Treaty on Legal Assistance in Criminal Matters between China and Brazil sets that the party being requested may provide the assistance under a negotiated scope (not using requirement for dual criminality), regardless whether the action constitutes a crime under its domestic law.

Criterion 37.7 Dual criminality for the purposes of MLA shall be satisfied regardless of whether both countries place the offence within the same category of offence, or denominate the offence by the same terminology as long as both countries criminalize the conduct underlying the offence (treaties on MLA between China and other countries).

Criterion 37.8 Chinese competent authorities dealing with requests for criminal legal assistance can use the powers and investigative techniques consistent with the handling of domestic cases which are extensive depending on the nature of requested actions. These investigative powers and techniques can be used for regular LA requests, but also for requests directly from foreign judicial or law enforcement

Interpretations of the Supreme People's Court on – Š ‡ ’ ’ Ž ‹ … ƒ – ‹ • ‘ ˆ ” ‹ • ‹ • ƒ Ž ” ‘ … ‡ † — ” ‡ ƒ ™ ‘ ˆ , Arts. 410; ‡ ‘ ’ Ž ‡ ï • ‡ ’ — „ Rules of Criminal Procedure of the People's Procuratorate, Arts. 679 and 693; Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies, Articles 365, 367, and 368).

See R.31 for an overview of the available investigative powers and techniques for MLA.

Weighting and Conclusion

China has a sound system and rules for mutual legal assistance. Despite the clear procedures for dealing with foreign requests, there are no requirements for prioritization of them. China relies on the indication by the requesting party of the urgency of requests. There is no legal provision requiring that fiscal and confidentiality issues cannot be grounds for refusal. Although China insists on using dual criminality as a condition for providing mutual legal assistance it can, in

ïð - ñòò ëéóô

In its Third Round MER, China was rated largely compliant with these requirements. The main deficiency identified was the absence of a formal legal basis for equivalent value confiscation as an obstacle to the execution of foreign MLA requests based on such orders. There have been changes to the Recommendation since the Third Round MER.

Criterion 38.1 Requests to take seizing or confiscation action must be based on a bilateral treaty or multilateral convention that has been concluded or signed by China, or on the principle of reciprocity. All types of property and instrumentalities are covered in China (Criminal Law, Art. 64). As with other MLA issues, the MOJ has been designated as the competent authority to handle requests based on multi- or bilateral

treaties (see c.37.2 above). Diplomatic channels must be used when no such treaty or convention exists.

Beyond the legal provisions and procedures that apply for any MLA requests (see R.37), there are no additional legal provisions or procedures to expedite foreign freezing, seizure, and confiscation requests.

There is no legal provision for executing equivalent value seizures and confiscation requests in China (see R.4 above).

Criterion 38.2 There are no specific authority or procedures for providing MLA to requests made on the basis of foreign non-conviction-based confiscation proceedings except in cases when the criminal suspect or defendant escapes and cannot be present in court after being wanted for a year (including being missing), or a criminal suspect or defendant dies. If his or her illegal proceeds and other property involved in the case are to be recovered in accordance with the Criminal Law, a People's Procuratorate may file an application to a People's Court for confiscation of illegal proceeds. However, such application could not be triggered by an MLA request without a pro forma domestic investigation or procedures (CPL, Arts. 280 283; Provisions of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of the Confiscation Procedures for Illegal Proceeds in a Case Where a Criminal Suspect or Defendant Escapes, Hides, or Dies).

Criterion 38.3 The arrangements for coordinating seizure and confiscation actions with other countries are those provisions that regulate all MLA (see R.37) and specific arrangements in bilateral agreements with other countries (e.g., Agreement between the Government of the United States and the Government of China on Mutual Legal Assistance in Criminal Matters, Arts. 14, 16).

The legal obligation for proper preservation of properties involved in criminal cases that are seized, frozen, and confiscated are contained in Art. 130, CPL. The mechanism for the management and disposal of case properties, which includes the system for retention of case properties and procedures for the management of properties in advance, to manage, when necessary, the frozen, seized, or confiscated property is set in Opinions on Further Regulating the Disposition of Property Related to Criminal Proceedings (issued by the General Office of the CPC Central Committee and the General Office of the State Council), Provisions on the Management of Property • ˜ ‘ Ž ˜ ‡ † ‹ • ” ‹ • ‹ • ƒ Ž ” ‘ … ‡ ‡ † ‹ • ‰ • „ › ’ ‡ and Provisions of the ƒ – ‘ ” ƒ – ‡ • á Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security, the Ministry of Justice, and the Legislative Affairs Commission of the Standing Committee of the National People's Congress on Several Issues concerning the Implementation of the Criminal Procedure Law (Art. 10 of Handling of Property Involved in a Case).

Criterion 38.4 Where a criminal case is solved through international co-operation, the Chinese government may share with the cooperative countries the illegal gains, the proceeds thereof, the property used for the drug-related crimes or the money from selling such property (Narcotics Control Law, Art. 57).

China and other countries can share confiscated properties under provisions of agreements. For example, in 2016, China and Canada signed Agreement between – Š ‡ ‘ ˜ ‡ ” • • ‡ • – ‘ ^ – Š ‡ ‡ ‘ ’ Ž ‡ ï • ‡ ’ — „ Ž ‹ … ‘ ^ Š ‹ • ƒ ƒ • † – Š ‡ ‘ ˜ ‡ ” • • ‡ Sharing and Return of Recovered Assets. The agreement stipulates that the illegally

Anti-

Weighting and Conclusion

The extradition regime of China is solid and well organised. The main deficiency i

Tax Collection (Art. 91) stipulates that the Chinese government can conclude taxation treaties with foreign jurisdictions to engage in international co-operation.

C.40.2b Competent authorities are not prevented from using the most efficient means possible for providing assistance. Competent authorities have entered into numerous MOUs or bilateral and multilateral agreements with other foreign entities to facilitate cooperation. This information sharing agreements cover a broad range of foreign counterparts from numerous jurisdictions.

C.40.2c There are clear and secured information exchange channels for the transmission and reception of foreign requests during international co-operation. The CAMLMAC has established its International Anti-Money Laundering Information Transmission System (CSW), which is dedicated to exchanging information with foreign FIUs. Art. 5 of the Processing Procedures of AML and Analysis Centre provides that in addition to the CWS System, e-mails, letters, and faxes can be used for international information exchange. As of April 2018, it signed MOUs or similar cooperative documents with FIUs of 50 countries. Other competent authorities also sign MOUs to facilitate the exchange of information. They conduct information exchange with overseas parties through various channels. Non-confidential intelligence can be delivered via Internet email; while confidential intelligence shall be exchanged through encrypted networks, encrypted faxes or special channels. The PBC has signed MOUs with a number of jurisdictions including Russia, Argentina, and Macau, China, to facilitate international cooperation, including the exchange of information. The Ministry of Public Security has established close cooperation relationships with 113 countries, established 129 bilateral and multilateral cooperation mechanisms and 96 liaison hotlines, sent 72 police liaison officers to 35 countries, and signed nearly 400 co-operation documents with the internal police department of more than 70 countries.

C.40.2d Clear standard procedures have been established for international co-operation with foreign counterparts, but the processes for the timely prioritisation of the execution of requests have not been established. The Procedures for Processing of Foreign Intelligence Information Documents of the CAMLMAC clarify the processing procedures for the exchange of intelligence with foreign counterparts by mentioning

State Administration of Taxation in its Rules for the International Exchange of Tax Information. In practice, the priority is decided at the beginning of dealing with requests. There is no information on other authorities.

C.40.2e Various competent authorities have processes and procedures for safeguarding information received from foreign counterparts. The legal documents have provisions on safeguarding the confidentiality of information received by them.

Criterion 40.3 The Chinese government can carry out international cooperation in AML, CFT, and related fields in accordance with international treaties concluded or acceded to, or in accordance with the principle of equality and reciprocity. Thus, while generally multilateral or bilateral agreements are welcome, they are not required conditions for competent authorities to carry out international cooperation (AML Law, Art. 27). CAMLMAC can only exchange information with counterpart FIUs based on a formal cooperation agreement, and it does not engage in the exchange of information exclusively based on confidentiality and reciprocity.

Competent authorities of China have negotiated with a wide range of foreign counterparts and signed cooperation agreements. For instance, the PBC has signed memoranda of cooperation with four jurisdictions (Argentina, Australia, Macau, China, and Russia). The CAMLMAC has signed MOUs on information exchange with 50 countries, the General Administration of Taxation has signed a number of international treaties on tax cooperation on behalf of the Chinese government. The conclusion of agreements is done in a timely manner.

Criterion 40.4 In accordance with international custom, after requesting information and obtaining responses from foreign counterparts, some Chinese competent authorities will provide feedback on the use and usefulness of the information to the foreign counterparts.

The State Administration of Taxation expresses its gratitude to foreign counterparts for the information that has brought significant amount of tax for China indicating the amount of taxes.

Criterion 40.5 Chinese competent authorities exchange information or provide assistance in accordance with the laws or with the treaties, agreements, or according to the principles of equality and reciprocity (AML Law, Arts. 27, 28). There is no information suggesting that laws place unreasonable or unduly restrictive conditions, but they do not specifically allow international co-operation in the cases covered by c.40.5 in the Methodology. The information received from the Global Network points to a number of international requests for information that have not been honoured without supporting feedback from the Chinese authorities. The authorities stated that the information request of a foreign authority will not be rejected because of the involvement of fiscal matters, issues of confidentiality, active inquiry or investigations (with reasonable exclusion of cases of possible impeding of investigations or prosecutions), or the status of the requiring authority.

Specific provisions for such situations is mentioned only for The State Administration of Taxation: it shall not reject providing intelligence to foreign counterparts for the following reasons: the information request has nothing to do with tax benefits of China; the tax authorities have the obligation to keep the taxpayer information confidential; the bank has confidential obligation with the information of the depositor; the tax information is controlled by an agent, an intermediary, or other third parties etc. (Rules for the International Exchange of Tax Information, Art. 10).

Criterion 40.6 The PBC, CAMLMAC, and tax authorities have controls and safeguards in place to ensure that information exchanged is only used for its intended purpose. The Ministry of Public Security, for example, includes such provision in its MOUs with LEA of other countries. When the CAMLMAC requests intelligence from foreign counterparts, it explicitly states the purpose of using the information. If the intelligence information provided by a foreign FIU is to be disclosed to the domestic LEAs, CAMLMAC requests the consent of the foreign counterpart (Standard Procedures for Processing of Foreign Intelligence Information Documents of the CAMLMAC, Arts. 13, 14; Law on the Administration of Tax Collection, Art. 54; Rules for the International Exchange of Tax Information, Chapter 3).

Criterion 40.7 Competent authorities maintain and protect the confidentiality of information exchanged, consistent with the relevant applicable legal provisions (Standard Procedures for Processing of Foreign Intelligence Information Documents of

the CAMLMAC, Arts. 13, 14; Law on the Administration of Tax Collection, Art. 54; Rules for the International Exchange of Tax Information, Chapter 3) and the terms of MOUs and [illegible]

supervision with four jurisdictions, which enables China to exchange AML supervisory information with counterparts in other jurisdictions.

Criterion 40.14 For the AML/CFT purpose, the PBC can exchange domestically available information specified in sub-criteria 40.14 (a) to (c) including supervisory information on AML and financial regulation with foreign counterparts, regardless of whether they are supervising the same group of financial institutions (AML Law, Art. 27; Counter Terrorism Law, Art. 68). However, since there are deficiencies in collecting and maintaining BO information (see R.24), and financial institutions are only required to take reasonable measures to identify BOs (see R.10), it is likely that PBC will not be always be able to share BO information with other supervisors.

Criterion 40.15 The PBC can carry out international AML/CFT cooperation, but the law describes in general its powers to cooperate and exchange relevant information, and is silent on the power, at the request of the foreign counterparts, to investigate AML/CFT information and provide feedback (AML Law, Arts. 27 28, CT Law, Art. 68). Based on the bilateral agreements or on the principle of reciprocity, Chinese regulators may authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in China.

Criterion 40.16 The PBC should explicitly state the purpose of information (e.g., for supervision only) when requesting supervisory information from foreign supervisors. If the information needs to be disclosed to other parties or used for other purposes, the PBC will obtain prior authorisation from the information providers. In accordance with the terms of cooperation agreements (where in place), the preliminary consent to disclose information is required.

Exchange of Information between Law Enforcement Authorities

Criterion 40.17 The law enforcement authorities of China carry out international cooperation with foreign law enforcement authorities according to international treaties of China, or under the principle of equality and reciprocity, and exchange information on ML, relevant predicate offences, and TF with foreign law enforcement authority, including the tracking and searching of criminal proceeds although the absence of provisions in law for confiscating property of corresponding value might present certain limitations to the cooperation (Counter Terrorism Law, Art. 68; Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies, Art. 364).

Police Cooperation. Public security authorities can cooperate with foreign police authorities to carry out police cooperation, including the exchange of criminal intelligence, investigation and evidence collection, service of criminal proceedings documents, transfer of evidence, documentary evidence, audio-visual materials or electronic data and other evidence, extradition, arrest and deportation of suspects, defendants, or criminals, as well as other criminal legal assistance and police cooperation stipulated in the international treaties and agreement (Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies, Art. 365).

Prosecution cooperation. As of September 2017, the Supreme People's Procuratorate has signed 146 co-operation agreements, MOUs, and other documents with 96 countries and regions. The content involves the cooperation in combating crimes, information exchange and personnel training etc.

Criterion 40.18 In police cooperation, the public security agencies of China can use the same investigative powers, techniques, and coercive measures as investigating domestic cases, and upon the requests from foreign counterparts, can inquire and obtain information on behalf of foreign counterparts (Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies, Art. 368).

When the Chinese LEAs and international organisations or foreign LEAs sign multilateral/bilateral cooperation agreements, parties agree on the use of information exchange. When a Chinese LEA requests information from a foreign counterpart, it will clearly indicate the purpose of using the information; if the information needs to be disclosed to other agencies or used for other purposes, prior authorisation will be sought from the requested party. For instance, the multilateral cooperation agreements signed by the Ministry of Public Security (such as through Interpol to inquire data, investigate and collect evidence) and bilateral police co-operation agreements also govern the restrictions on the use of information exchange.

Criterion 40.19 On the basis of multilateral and bilateral agreements, China can cooperate with other countries to carry out law enforcement joint action. For instance, since 2011, according to a joint statement of China, Laos, Burma, and Thailand, under the framework of the security cooperation mechanism among the four countries, the law enforcement agencies of China and the other three countries carry out the Mekong joint patrol enforcement to prevent, combat, and investigate crimes in Mekong River basin.

Exchange of Information between Non-Counterparts

Criterion 40.20 China allows domestic and foreign non-counterparts to exchange information indirectly under existing international cooperation mechanisms, but this is limited to agreements or MOUs concluded by China (for police cooperation Provisions on the Procedures for Handling Criminal Cases by Public Security Agencies, Art. 364, 367). For instance, foreign police trying to obtain information on financial supervision of China can make a request to the Ministry of Public Security which will transfer the request to the appropriate financial supervisor. The information from the financial supervisor will be provided through the Ministry of Public Security. Similarly, a foreign FIU can send a request to the CAMLMAC upon the request of their domestic police and transfer the information from the CAMLMAC to the police. The AML Law itself requires coordination among ministries and agencies in their AML work.

According to concluded international agreements and MOUs (for example, the MOU between the PBC and AUSTRAC), the Chinese authorities exchange information with foreign counterparts making it clear for what purpose and on whose behalf the request is made

Weighting and Conclusion

Competent authorities are generally able to provide a wide range of direct and indirect international assistance, with only minor deficiencies (no prioritization process, feedback not used by the FIU).

.

	x recent designation of DNFBPs and the lack of oversight DNFBPs in terms of AML/CFT obligations. In addition, assessment of risk by DNFBPs of their products nor clients been made. x There is currently no effective oversight or monitoring to ensu that DNFBPs are implementing their obligations under R.1. x DNFBPs have not been designated under the AML Law therefore are not subject to AML/CFT risk assessm obligations. x Payment institutions are not subject to a general requirement have policies, controls and procedures approved by se management to enable them to manage and mitigate identifi risks.
	x The Recommendation is fully met
	x Arts. 191 and 312 of the PC criminalising ML do not c x China follows the all-crimes approach under Art. 312 of the P however provinces and autonomous regions can also pla value range to determine if the behaviour is criminal. x Some of the predicate offences under Art.312 of the PC are narrow. x Self-laundering is not criminalised in China. x Prison sanctions are proportionate compared to other financ crimes, but low compared to the penalties for some of the main predicate offences that the third-party ML criminalisation aims to deter. x Legal entities are not criminally liable and it is unclear if sancti for legal persons are proportionate and dissuasive.
	x The Recommendation is fully met
	x The wording of the TF offence in Art. 120A of the PC is general and lacks the level of detail of the TF Convention, w makes it somewhat difficult to assess the requirements. x Not all required conduct listed in three Conventions Annexed the TF Conventions has been criminalised as terrorist condu x With respect to the terrorist related offences mentioned in th Annex of the TF convention there are three conventions whe not all conduct, has been criminalised as terrorist conduct. x Art. 120A of the PC seems to cover only direct assistance an the wilful collection of funds. x There are no legal provisions that prohibit legal persons a entities from makin62.14 99.384 86.304ET EMC u0.7 T9akis

- There are no legal provisions or mechanisms that ensure authorities operate against entities designated by th UNSCR or against entities to be proposed to the UN, or agai entities designated upon a foreign request or a domes proposal.
- The freezing requirements in the Counter Terrorism Law an Notice 187/2017, are incomplete in scope and only apply to and designated DNFBPs.

	by, or actively supporting, terrorist activity, or terrorist organisations.
	x The Recommendation is fully met
	x Payment institutions are not required to undertake CDD measures when carrying out occasional transactions in several operations that appear to be linked for a total exceeding the equivalent of USD/EUR 15 000. x Payment institutions are not required to verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person. x FIs are not explicitly required to identify the natural person who ultimately owns a customer that is a legal person or a legal arrangement. x There is no explicit requirement for payment institutions to ensure that documents, data, or information collected under the CDD process is kept up-to-date and relevant. x For customers that are legal persons or legal arrangements, the business and its ownership and control structure but requirement seems to be unduly limited to taking reasonable measures. x There is no requirement to collect information on the place of business of legal arrangements. x For life and other investment-related insurance policies where the beneficiary is designated by characteristics or by class or by other means, insurance institutions are not required to obtain sufficient information on the beneficiary to be able to establish the identity at the time of the pay-out. Measures of verification of the identity of the beneficiary are subject to thresholds and limited to specific types of payments. x FIs are not required to take enhanced measures, beyond enhanced customer identification measures, if they determine that a beneficiary who is a legal person or a legal arrangement presents a higher risk. x It is unclear whether the requirements governing the situations where low-risk customers are allowed to utilise the business relationship prior to verification are mandatory. x The requirement to supplement or update CDD information of existing customers is not based on materiality, nor should be done at appropriate times. x The implementation of CDD for existing relationships of payment institutions is not required on the basis of materiality and risk, and at appropriate times. x It is not clear whether the requirement to apply enhanced measures in situations where ML/TF risks are high are mandatory.
	x The Recommendation is fully met
	x There are no requirements for the use of risk management systems to determine whether a beneficial owner is a PEP. x It is not mandatory for FIs to take reasonable measures to establish the source of wealth of PEPs or conduct ongoing monitoring of business relationships with foreign PEPs.

	x Payment institutions are not explicitly required to have an ongoing training program and an independent audit function. x Payment institutions are not required to appoint a compliance officer at the management level and apply screening procedures to ensure high standards when hiring employees. x Financial institutions are not explicitly required to implement group-wide programs against ML/TF, including group-wide screening procedures when hiring employees and an ongoing employee training programme. x Payment institutions are not required to implement group-wide programs against ML/TF. x If the host country does not permit the proper implementation of financial groups are not explicitly required to apply appropriate additional measures to manage the ML/TF risks.
	x The Recommendation is fully met

- The verification of the registered information on LLCs and JS

	x Sanctions are not in line with the standards set out in R.35.
	x There are no measures for regulation and supervision of DNFBP except for trust companies and DPMs. This scope issue ha impact on all aspects of R.28.
	x centre for the receipt and analysis of STRs and other informa relevant to ML, associated predicate offences and TF; and fo dissemination of the results of that analysis. x The FIU compone ts face limitations in terms of operational an strategic analyses, which use available and obtaina information, because of the stand-alone databases at the leve of the PBC provincial branches and the limited access by t base. x The provincial branches require the signature of the presiden their branch for disseminations to competent authorities. T requirement out its functions freely and its operational independence and autonomy. x China did not file an unconditional application for Egmont Gro membership.
	x The Recommendation is fully met
	x The Recommendation is fully met
	x any currency and other types of BNI in foreign currency. T with each of the individual criteria of R.32. x The relevant information that the FIU receives from the custo authorities only covers declaration violation cases of exces amounts and does not specifically extend to false declarati nor suspicions of ML and TF. x Coordination and information sharing mechanisms are in an e implementation stage.
	x While statistics are largely kept on the four main areas covered by R.33, China was not always able to breakdown the statis into meaningful sub-components and at times needed to rely o samples.
	x There is no guidance for online lending institutions. x Guidance specifically directed to the provision of trustee servi does not appear to be issued. x DNFBPs, (aside from trust companies and DPMs) are not subje to the AML law and hence related guidance is not applicable
	x There are concerns that the sanctions applicable to the finan sector are not effective, dissuasive and proportionate given their low scale and cap compared to the size and composition of financial sector in China.

	x No sanctions applicable to designated DNFBPs.
	x Not all offences set out in the international conventions a offences under the Chinese law.
	x There are no clear processes for the timely prioritisation a execution of mutual legal assistance requests. x There is no legal provision requiring that fiscal and confidentia issues cannot be grounds for refusal. x Although China insists on using dual criminality as a condition providing mutual legal assistance it can, in particular situatio tance.
	x Beyond the legal provisions and procedures that apply for MLA requests (see R.37), there are no additional legal provis or procedures to expedite foreign freezing, seizure, a confiscation requests. x There is no legal provision for executing equivalent value seiz and confiscation requests in China. x There is no specific authority or procedures for providing MLA requests made on the basis of foreign non-conviction-based confiscation proceedings except in cases where the crimina suspect or defendant escapes (and cannot be present in c after being wanted for a year (including being missing)), c criminal suspect or defendant dies.
	x There are no procedures for simplified extradition.
	x Feedback from the Global Network suggests that it tal CAMLMAC on average between one to four months to prov foreign counterparts a response to their non-urgent information requests. This cannot be considered to be rapidly. x Relevant laws do not specifically provide for internatio cooperation in the cases covered by criterion 5 of R.40 in Methodology. Information received from the Global Netwo points to a number of international requests for information tha have not been honoured w ( )-6161.n 262. (w)-4 (( )-61631t

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
AMLB	Anti-Money Laundering Bureau
AMLD	Anti-Money Laundering Departments
AMLJMC	Anti-Money Laundering Joint Ministerial Conference
BO	Beneficial Ownership
CAMLMAC	China Anti-Money Laundering Monitoring and Analysis Centre
CBIRC	China Banking and Insurance Regulatory Commission
CCDI	Central Commission for Disciplinary Inspection
CDD	Customer Due Diligence
CIRC	China Insurance Regulatory Commission
CPC	Communist Party of China
CSP	Company Service Provider
CSRC	China Securities Regulatory Commission
DNFBP	Designated Non-Financial Businesses and Professions
DPM	Dealers in Precious Metals
ECID	Economic Crime Investigation Department
EEP	Electronic Enquiry Platform
ETIM	Eastern Turkistan Islamic Movement
FI	Financial Institution
FIU	Financial Intelligence Unit
GAC	General Administration of Customs
GDP	Gross Domestic Product
LEA	Law Enforcement Agency
LEI	Law on International Extradition
LVTR	Large Value Transaction Report
MCA	Ministry of Civil Affairs
MER	Mutual Evaluation Report
MFA	Ministry of Foreign Affairs
ML	Money Laundering
MLA	Mutual Legal Assistance
MOF	Ministry of Finance
MOJ	Ministry of Justice
MOHURD	Ministry of Housing and Urban-Rural Development

MOU	Memorandum of Understanding
MPS	Ministry of Public Security
MS	Ministry of Supervision
MSS	Ministry of State Security
NLGCT	National Leading Group for Countering Terrorism
NPC	National People's Congress
NPO	Non-profit Organization
NRA	National Risk Assessment
NSC	National Supervisory Commission
OECD	Organisation for Economic Co-operation and Development
PBC	
PEP	Politically Exposed Person
PI	Payment Institution
PF	Proliferation Financing
POC	Proceeds of Crime
PSB	Public Security Bureaus
SAIC	State Administration of Industry and Commerce
SAMR	State Administration for Market Regulation
SAR	Special Administrative Region
SAT	State Administration of Taxation
SGE	Shanghai Gold Exchange
SPC	
SPP	
STR	Suspicious Transaction Report
TCA	Technical Compliance Annex
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution

FATF APGML EAG

..a .- a| . . .a . . a . .

A . 2019

A - a a a | a a
P R . . C a

Fourth Round Mutual Evaluation Report

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in the People's Republic of China (China) as at the time of the on-site visit from 9 to 27 July 2018.

The report analyses the level of effectiveness of China's AML/CTF system, the level of compliance with the FATF 40 Recommendations and provides recommendations on how their AML/CFT system could be strengthened.