



**THE VTB GROUP CONSOLIDATED POLICY
ON THE PREVENTION OF MONEY LAUNDERING
AND TERRORIST FINANCING**

CONTENTS

THE VTB GROUP CONSOLIDATED POLICY	1
GENERAL PROVISIONS.....	3
DEFINITIONS.....	3
GENERAL PRINCIPLES AND COORDINATION WITHIN THE VTB GROUP.....	4
REPORTING AND ANALYSIS.....	5
MAIN RESPONSIBILITIES.....	5
AML OFFICER STATUS AND RESPONSIBILITIES.....	6
AML/CTF PROCEDURES	7
CUSTOMER DUE DILIGENCE	7
<i>Identification requirements for new personal customers.....</i>	<i>7</i>
<i>Politically Exposed Persons (PEPs).....</i>	<i>8</i>
<i>Identification requirements for corporate customers.....</i>	<i>8</i>
<i>Identification requirements for trusts, foundations and similar entities</i>	<i>9</i>
<i>Identification requirements for financial institutions.....</i>	<i>9</i>
<i>Further information about the non-bank customer.....</i>	<i>10</i>
<i>Updating customer files</i>	<i>11</i>
MONITORING CUSTOMER ACTIVITY	11
RISK-BASED APPROACH	12
REPORTING PROCEDURES	14
CONFIDENTIALITY	15
RECORDS KEEPING	15
TRAINING OF PERSONNEL.....	16
CLOSING PROVISIONS	17

GENERAL PROVISIONS

Financial institutions run legal, regulatory, reputational and as a consequence financial risks if they are used as vehicles for money laundering and terrorist financing.

The VTB Group Consolidated Policy on Prevention of Money Laundering and Terrorist Financing (hereinafter referred to as Policy) stipulates the general framework of internal AML/CTF control within the VTB Group in order to mitigate the above mentioned risks.

When implementing AML/CTF controls VTB Group Companies follow national laws and regulations and this Policy. National laws and regulations are to be applied if in conflict with any of the provisions of this Policy.

DEFINITIONS

Parent Bank	-	JSC VTB Bank;
VTB Group	-	JSC VTB Bank and financial institutions with JSC VTB Bank's participation in their authorized/share capitals exceeding 50% of the total voting shares/stakes, which are credit institutions (i.e. entities engaged in banking business) under applicable legislation of the country of their incorporation; or financial institutions (i.e. entities which are not credit institutions and are engaged in securities trading, insurance business or any other financial services; as well as management companies of mutual funds, leasing companies, or any other entities engaged in financial business) - "Subsidiary financial institutions". Subsidiary banks and Subsidiary financial institutions are jointly referred to as Subsidiary Companies;
VTB Sub-Holding	-	A group of companies united by territorial proximity and/or business specifics, with the participation of the Subsidiary Company (which is the Head Company of the Sub-Holding) in their share capital exceeding 50% of the total voting shares/stakes;
AML/CTF	-	anti-money laundering/counter terrorist financing;
AML/CTF internal control	-	Activities performed by VTB Group Companies aimed at anti-money laundering and counter terrorist financing;
AML Officer	-	Anti-Money Laundering Officer – an employee, who is responsible for implementation of VTB Group Company's AML/CTF internal regulative documents and for the conformity to the national AML/CTF laws and regulations;
Authorized body	-	National body (bodies) performing activities aimed at anti-money laundering and counter terrorist financing in accordance with the national legislation and receiving suspicious transactions reports and other reports sent by a VTB Group Company for compliance with national AML/CTF laws and regulations;

Customer	-	Any individual or entity who seeks to enter or has already entered into a business relationship, or conducts a one-off transaction, with a VTB Group Company, as principal or as an agent for someone else;
FATF	-	Financial Action Task Force, an intergovernmental body which sets standards, develops and promotes policies to combat money laundering and terrorist financing;
KYC	-	Know Your Customer;
ML/TF	-	Money laundering which means bringing a legal appearance to the possession, use or disposal of amounts of money or other property received as the result of committing an offence which is defined by the national legislation and/or terrorist financing;
National laws and regulations	-	Acts of law and regulations or guidance of national authorities which regulate/supervise AML/CTF activities of VTB Group Companies;
VTB Group Management Committee (VTB GMC)	-	Permanent collective body responsible for ensuring coordination along all business lines of VTB Group. Acting with its powers, VTB GMC aims to improve the efficiency of the VTB Group management, considers and makes decisions, concerned development strategy of the Subsidiary Companies and the VTB Group as a whole. VTB GMC functions and procedures are governed by the VTB GMC Regulation;
Politically Exposed Persons (PEPs)	-	Individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
Financial institution	-	A legal entity, which performs one or several types of activities, listed in the definition of "financial institution" term in the glossary to FATF 40 Recommendations.
Dormant account	-	A bank account on which no transaction has occurred for 6 months or more.

GENERAL PRINCIPLES AND COORDINATION WITHIN THE VTB GROUP

Wishing to unite their efforts in preventing involvement in money laundering or terrorist financing activities, VTB Group Companies agree to:

- follow general provisions and approaches in establishing and maintaining AML/CTF internal control systems mentioned in this Policy,
- tailor their own internal AML/CTF rules and procedures based on national laws and regulations and unify them (considering restrictions set by national laws) on the basis of VTB Group standards set by this Policy;
- take mutual actions to mitigate risks relating to money laundering or terrorist financing that shall be undertaken within each VTB Group Company and VTB Group as a whole;

- coordinate their efforts when elaborating measures aiming to prevent money laundering or terrorist financing;
- take part in sharing information in order to spread best practices in establishing and maintaining AML/CTF internal control;
- assist each other in solving problems relating to the functioning of AML/CTF internal control system or arising in connection with the implementation of AML/CTF internal control rules on a case by case basis.

In accordance with the FATF Recommendations the principles used by financial institutions to prevent money laundering should be also applied to branches and majority owned subsidiaries particularly those located in countries which do not fully comply with the FATF recommendations, are considered to have inadequate AML standards, insufficient regulatory supervision or present a greater risk of corruption, terrorist financing or crime.

REPORTING AND ANALYSIS

In order to ensure adherence to general principles of AML/CTF internal controls within the VTB Group, to maintain the soundness of AML/CTF system and to assess AML-related risks on a consolidated basis, VTB Group Companies forward information about the implementation of the AML/CTF rules and procedures to the Parent Bank quarterly.

Subsidiary Company's AML Officer is responsible for preparing and forwarding Subsidiary Company's reports to the Parent Bank.

The AML Compliance department of the Parent Bank is responsible for analyzing the reports and other information relating to the functioning of AML/CTF internal controls in the VTB Group Companies and for preparing consolidated reports to the management of the VTB Group on the effectiveness of the VTB Group AML/CTF strategy and existing money laundering/terrorist financing risks.

The results of the analysis of the Reports received from Subsidiary Companies and Head Companies of the Sub-Holdings are annually delivered to VTB Group Management Committee within the framework of annual reports.

MAIN RESPONSIBILITIES

When establishing and maintaining AML/CTF systems VTB Group Companies presume, that:

- they cannot contract out of their regulatory responsibilities, and therefore they remain responsible for their AML/CTF systems and controls,
- the responsibility for the establishment and maintenance of effective AML/CTF systems and controls rests with the senior management of the VTB Group Company, if not provided otherwise by national laws,
- a VTB Group Company implementing national AML/CTF law should have an AML Officer in its staff. An AML Officer should be appointed by the VTB Group Company's senior management decision or otherwise as stipulated by the local AML/CTF legislation. The Parent Bank is informed about a newly appointed AML Officer of a VTB Group Company.

- all staff should be fully aware and understand their legal and regulatory responsibilities and obligations with regard to money laundering and terrorist financing activities,
- information on the effectiveness of the VTB Group Company's AML/CTF rules in preventing money laundering and terrorist financing is regularly presented to the senior management of the VTB Group Company within the time-frame set by national laws and regulations,
- VTB Group Companies have internal AML/CTF documents approved by the country supervisory authorities (if necessary), including:
 - customer due diligence and monitoring customer's activities procedures,
 - risk management policies and risk profile in relation to money laundering and terrorist financing and application of those policies,
 - reporting procedures and data protection clauses,
 - record keeping provisions,
 - confidentiality provisions,
 - staff training procedures,
- the internal AML/CTF documents are regularly revised in order to follow the developments in national AML/CTF regulations, the emerging of new products and/or other changes in the VTB Group Company's business profile.

AML Officer STATUS AND RESPONSIBILITIES

A VTB Group Company implementing national AML/CTF law should ensure the appointment of an AML Officer with adequate seniority, experience and authority in order to act independently in carrying out his responsibilities. As a rule, the AML Officer heads the division of the Subsidiary Company, which is responsible for maintaining and developing the AML/CTF internal system of the Company. AML Officer can combine AML compliance duties with other responsibilities, if it does not contradict national legislation. Combining different responsibilities by this employee should not lead to the conflict of interests and interfere with his making independent decisions on AML/CTF issues.

Companies of the VTB Sub-Holding, which are subject to implementing national AML/CTF legislation, can delegate performing AML Officer responsibilities to the AML Officer of the VTB Sub-Holding Head Company, if it does not contradict existing AML/CTF laws and regulations implemented in the country (territory) of a company's registration.

The AML Officer is responsible for the VTB Group Company's compliance with the national AML/CTF legislation, internal rules and procedures and this Policy as well as for developing AML/CTF internal rules and procedures and for presenting them to the governance bodies of the VTB Group Company for approval.

The AML Officer is further responsible for organizing the procedure of reporting to the Authorized body. It is also his responsibility to respond promptly to any reasoned request for information made by this body, national supervisory or law enforcement authorities.

The AML Officer reports annually to the senior management of the VTB Group Company on the effectiveness of the Company's AML/CTF strategy and existing money laundering/terrorist financing risks. This information shall also be brought to the notice of the AML Officer of the Parent Bank.

AML/CTF PROCEDURES

CUSTOMER DUE DILIGENCE

VTB Group Companies take necessary measures to be reasonably satisfied that their customers are who they say they are, as well as to understand that there is no legal barrier to providing them with the product or service requested.

VTB Group Companies should take necessary measures to recognize the persons (individuals and legal entities) to whom financial sanctions of national or international bodies apply in order to refrain from entering into a business relationship or conducting a one-off transaction with such persons.

The identity of a prospective customer is not verified in cases provided by the national laws and regulations unless the Company knows or suspects that a proposed relationship or a one-off transaction involves money laundering or terrorist financing.

VTB Group Companies also take reasonable measures to establish, whether the customer is acting for another person or entity and to identify persons to whose advantage the customer acts, except in situations specifically exempted by national laws and regulations.

VTB Group Companies do not open accounts for anonymous customers.

Satisfactory identification of the customer takes place as soon as reasonably practicable after first contact between the Company and the customer. Business could be conducted before satisfactory identification evidence has been obtained only in exceptional cases allowed by national laws or regulations and approved by the management of the VTB Group Company as appropriate. In such circumstances, Company's risk management procedures require controls to be placed over the extent of the relationship entered into, or any funds held under the relationship, until verification has been completed.

In identifying a customer, the Company obtains a range of information from the customer and verifies this information (or some of it) through the use of reliable, independent source documents, data or information.

Identification requirements for new personal customers

In identifying an individual, the Company obtains the following information:

- full name,
- residential address,
- date and place of birth,
- identification documents,
- other information required by national laws and regulations.

The obtained information is verified either on the basis of a document (documents) produced by the customer, or electronically by the Company (if such a possibility exists under national regulations), or by a combination of both. Where business is conducted face-to-face, the Company employees have to require originals of any documents involved in the verification and takes copies (where possible). Where it is not possible to take copies of original documents, a file note is made confirming what original documents were sighted to evidence the customers' identity.

Documentary verification of customer's identity is accomplished only on the basis of documents considered as evidences of identity by national laws and regulations.

If identity is verified electronically, this should be on the basis of the customer's full name, date of birth and other criteria, set by national laws and regulations.

Politically Exposed Persons (PEPs)

As regards Politically Exposed Persons, in addition to the standard evidence obtained about an individual VTB Group Companies:

- determine, using a risk-based approach, whether a customer is a PEP;
- obtain appropriate senior management approval for establishing or maintaining business relationships with such customers;
- take reasonable measures to establish the source of wealth and source of funds of such customers; and
- conduct enhanced ongoing monitoring of the financial activities of a PEP.

It is recommended to accept those individuals who belong to the category of politically exposed persons as customers upon the receipt of the Company's management approval. The Company's management can delegate the decision-making on this issue to the level of the Head of the Company's division, which will service a PEP, or to the AML Officer, provided that this is allowed by the national law.

New and existing customers may not initially meet the definition of a PEP. VTB Group Companies should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure.

Identification requirements for corporate customers

VTB Group Companies take necessary measures to ensure that they fully understand the corporate customer's legal form, structure and ownership, and obtain sufficient additional information on the nature of the company's business, and the reasons for seeking the product or service.

VTB Group Companies obtain the following information in relation to the legal entity concerned:

- full name,
- registered number,
- registered address in country of incorporation,
- business address, place of central management and administration,
- tax identification number,
- list of administrative bodies and all directors (or equivalent),
- other information required by national laws and regulations.

It is a part of the VTB Group Company's procedures to know the names of all beneficial owners of non-personal customers holding 20% of capital or more. However, if national laws and regulations require to identify beneficial owners holding less than 20% or the VTB Group Company's assessment of the money laundering or terrorist financing risk presented by the customer is high, it may be decided to verify the identities of beneficial owners holding less than 20%.

Corporate customers that are listed on a regulated market are publicly owned and generally accountable. After satisfying itself that the customer is a publicly quoted company, there is no need of further steps to verify identity of the customer over and above obtaining the standard evidence mentioned above, if national laws and regulations permit so.

VTB Group Companies have to verify the identity of the intermediary and, if the intermediary acts for another, the identity of the underlying customer with the exceptions (if any) made by national regulations.

For operational purposes, the Company should have a list of those authorized to give instructions for the movement of funds or assets, along with an appropriate instrument authorizing one or more directors (or equivalent) to give the Company such instructions. The identities of individual signatories need only be verified on a risk-based approach unless the national laws and regulations provide that all authorized signatories should be identified.

Identification requirements for trusts, foundations and similar entities

In addition to the standard evidence obtained about corporate customers VTB Group Companies obtain the following information in respect of trusts, foundations and similar entities:

- nature and purpose of the trust, foundation or similar entity,
- country of establishment,
- name and address of any protector or controller,
- other information required by national laws and regulations.

VTB Group Companies identify all trustees, settlors, founders, beneficiaries and other persons who have authority to operate an account or to give the VTB Group Company instructions concerning the use or transfer of funds or assets following the identification procedure for individuals or legal entities as the case may be.

VTB Group Companies take appropriate steps to be reasonably satisfied that the person the Company deals with is properly authorized by the customer and is who he says he is.

Identification requirements for financial institutions

When establishing correspondent relations with financial institution the following elements are considered to be appropriate:

- full name and registration details (registered number and date of registration),
- the jurisdiction where the financial institution is incorporated (headquartered) and where its operating unit wishing to maintain the relationship with the VTB Group Company conducts its business, registered and business addresses,

- the legal form, ownership and executive management of the financial institution (including information about existence of any PEP in the executive management or ownership structure),
- the types of financial products and services the financial institution is offering and the markets these products and services are offered to,
- the types of products and services the financial institution wishes to obtain by establishing correspondent relations,
- general information about the financial institution's history,
- AML/CTF measures applied by the financial institution.

Unless national laws and regulations as well as internal procedures of the VTB Group Company provide otherwise, before establishing a relationship with a financial institution the Company forwards AML Questionnaire to a financial institution where the risk assessment of money laundering for the financial institution or country where that financial institution is domiciled is considered high. VTB Group Companies use the Questionnaire form as per Appendix to this Policy, which can be amended by additional questions and provisions. As a supplementary tool in obtaining information on a financial institution the use of Due Diligence Repository of Banker's Almanac (www.bankersalmanac.com) is recommended.

VTB Group Companies shall not establish correspondent relationships with financial institutions that have no AML/CTF controls. This rule applies to foreign financial institutions incorporated in Non Cooperative Countries and Territories defined by FATF.

VTB Group Companies shall not establish relationships with shell banks or with institutions acting on their behalf.

If a financial institution obtaining correspondent banking services provides itself such services to other financial institutions, reasonable steps shall be taken to understand the business of financial institutions which receive such services from the customer financial institution.

The detailed identification and verification procedures for new financial institutions may vary depending on the country of incorporation of the financial institution, if national laws and regulations permit so. However, as a general rule, VTB Group Companies shall have documentary evidence of:

- the existence of the institutions they intend to establish relationships with,
- a license or other evidence, which confirms that the institution is centrally regulated/supervised in the home country by the regulatory body,
- any other information as required by national laws and regulations.

Further information about the non-bank customer

In order to exercise a risk-based approach more thoroughly, it is recommended that additional information is obtained to the standard evidence which is obtained for the verification of the customer's identity, including some or all of the following:

- nature and details of the business/occupation/employment;
- record of changes of address;

- the expected source and origin of the funds to be used in the relationship;
- whether the expected business be transacted for own or not only for own account (fiduciary business),
- initial and ongoing source(s) of wealth or income (particularly within a private banking or wealth management relationship);
- copies of recent and current financial statements;
- the relationship between signatories and beneficial owners;
- the anticipated level and nature of the activity that is to be undertaken through the relationship;
- the purpose and reason for opening the account or establishing the relationship.

In practice, under a risk-based approach, it is not appropriate to know customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. VTB Group Companies' information demands need to be proportionate, appropriate and discriminative.

VTB Group Companies should hold a fuller set of information in respect of those customers, or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, as well as of those who seek a product or service carrying a higher risk of being used for money laundering or terrorist financing purposes.

Updating customer files

It is strongly recommended within the VTB Group, that VTB Group Companies take steps to ensure that they hold appropriate up-to-date information on their customers. In order to keep the information about customers up to date, the VTB Group Companies review and update existing customer records not less frequently than once every three years. The review and updating for high-risk customers is performed at least once a year. In addition, a review and update of the customer's records could be performed, if considered necessary, when a transaction of significance takes place (i.e. renewal of facilities, opening of a new account), or when any changes occur in customer's regulatory status, ownership structure, risk profile, etc.

MONITORING CUSTOMER ACTIVITY

Having regard to:

- the general requirement to establish appropriate procedures of internal control for the purposes of forestalling and preventing money laundering/terrorist financing and
- the requirement to report knowledge or suspicion of possible money laundering/terrorist financing and to report cases falling under mandatory control transactions (in some jurisdictions), VTB Group Companies establish and maintain an appropriate approach to enable them to detect transactions or activity that may raise suspicions for money laundering or terrorist financing as well as to detect mandatory control transactions (in appropriate jurisdictions).

In addition to carrying out customer due diligence and exercising KYC policies, VTB Group Companies monitor customer activity with a view to identify, during the course of a relationship, unusual activity. If unusual events cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions throughout a relationship helps to

give greater assurance that the Company is not being used for purposes of money laundering or terrorist financing.

The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- the reports on these transactions and/or activities are reviewed promptly by the authorized person(s); and
- appropriate action is taken if the findings of such further examination so warrant.

Monitoring can be executed:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
- after the event, through some independent review of the transactions and/or activities that a customer has undertaken.

In both cases, unusual transactions or activities are flagged for further examination.

The monitoring procedures include types of customer's transactions, the profile of the customer, comparison of the customer's activity and profile with that of a similar, peer group of customers.

It is also recommended, that VTB Group Companies have systems and procedures to deal with customers who have not had contact with the Company for some time, in circumstances where regular contact might be expected, and with dormant accounts or relationships, in order to be able to identify future reactivation and possible unauthorized use.

In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume, size and character of transactions with customers, in the context of the assessed customer and product risk.

Monitoring systems can be manual and/or automated. However, it is essential to keep the staff of VTB Group Companies alert, since such factors as staff intuition, direct exposure to a customer face-to-face or on the telephone, and the ability, through practical experience, to recognize transactions that do not seem to make sense for that customer, cannot be automated.

RISK-BASED APPROACH

By implementing a reasonably designed risk-based approach, VTB Group Companies identify the criteria to measure and mitigate potential money laundering and terrorist financing risks.

To assist the overall objective to prevent money laundering and terrorist financing through VTB Group, a risk-based approach:

- recognizes that the money laundering/terrorist financing threat varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;

- allows senior management to apply its own approach to the Company's procedures, systems and controls and arrangements in particular circumstances; and
- helps to produce a more cost effective AML/CTF system.

A risk-based approach takes a number, or all, of the following steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the Company:

- identify and assess the money laundering and terrorist financing risks that are relevant to the Company;
- design and implement controls to manage and mitigate the assessed risks;
- monitor and improve the effective operation of these controls.

In identifying and assessing the above mentioned risks, the VTB Group Companies determine and use their own procedures and criteria considering that the general trends of assessment include:

- customer base;
- products and services offered by the Company;
- delivery channels used by the Company;
- geographical areas of the Company's operation.

As regards money laundering and terrorist financing, managing and mitigating the risks will involve measures:

- to verify the customer's identity;
- to collect additional KYC information about the customer, and
- to monitor his transactions and activity, to determine whether there are reasonable grounds for knowing or suspecting that money laundering or terrorist financing may be taking place.

VTB Group Companies decide, on the basis of their assessments of the risks posed by different customer/product combinations, the level of verification that is applied at each level of risk presented by the customer. Consideration is given to all the information gathered about a customer, as part of the normal business and vetting processes. Consideration of the overall information held may alter the risk profile of the customer. Certain jurisdictions are recognized internationally as having inadequate Anti-Money Laundering standards, lacking regulatory supervision or presenting a greater risk of corruption, crime or terrorist financing. Others, such as many members of FATF, have more robust regulatory environments, which present lower risks.

To assess that risk mitigation procedures and controls are working effectively, the VTB Group Companies' internal AML/CTF procedures will need to be kept under regular review with the following aspects to consider:

- appropriate procedures to identify changes in customer characteristics, which come to light in the normal course of business;

- reviewing ways in which different products and services may be used for money laundering/terrorist financing purposes, and how these ways may change;
- adequacy of staff training and awareness;
- monitoring compliance arrangements (such as internal audit/quality assurance processes or external review);
- the balance between technology-based and people-based monitoring and assessing systems;
- capturing appropriate management information;
- upward reporting and responsibility;
- effectiveness of liaison between AML Compliance department of the Company and other Company departments; and
- effectiveness of the liaison with regulatory, supervisory and law enforcement agencies.

Risk management generally shall be regarded as a continuous process, carried out on a dynamic basis. VTB Group Companies therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review. It is recommended that the Companies revisit their assessments at least annually. Details of the assessment and any resulting changes should be included in the AML Officer's annual AML/CTF report.

REPORTING PROCEDURES

There are two types of transactions, which are to be reported to the Authorized body:

- transactions subject to mandatory control according to national laws and regulations, and
- transactions and activities, in respect to which knowledge, suspicion, or reasonable grounds for knowledge or suspicion exist, that a person is engaged in money laundering, or terrorist financing.

Following the differences in national legislations, VTB Group Companies have dissimilar scope of responsibilities with regard to reporting transactions and activities.

However, the following core obligations are part of reporting procedures of all the VTB Group Companies:

- all staff participates in raising information about transactions, which are subject to reporting procedures,
- the Company's AML Officer considers all internal reports on transactions subject to reporting procedures,
- the Company's AML Officer makes an external report to the Authorized body within the period of time stipulated by the law, or as soon as it is practicable, if there are no special provisions in national legislation,
- suspicious approaches are also reported, even if no transaction takes place,
- all actions in respect of transactions subject to reporting procedures are to be documented and retained under regular review,

- the details of transactions which are subject to reporting procedures and all correspondence exchanged with the authorities in relation to these transactions are documented,
- the external reports to the Authorized body should contain as much information about the customer, transaction or activity as is determined by national laws and regulations.

CONFIDENTIALITY

The information about customers and their transactions obtained in the course of fulfilling AML/CTF internal control is considered as confidential.

The employees of VTB Group Companies should not disclose to other persons the AML/CTF ways and means implemented by the Company.

The “tipping off” is strictly prohibited.

RECORDS KEEPING

VTB Group Companies keep records, including:

- customer information,
- transactions,
- internal and external reports about suspicious and mandatory control transactions,
- AML Officer annual (and other) reports,
- information not acted upon,
- training and information about the effectiveness of training, containing, in particular:
 - dates AML/CTF trainings were given,
 - the nature of the training,
 - the names of the staff who received training; and
 - the results of the tests undertaken by staff, where appropriate,
- compliance monitoring containing, in particular:
 - reports by the AML Officer to senior management; and
 - records of consideration of those reports and of any action taken as a consequence.

Records concerning customer identification and transactions are kept as evidence of the work that the Companies have undertaken in compliance with their legal and regulatory obligations, as well as for use as evidence in any investigation conducted by law enforcement.

Records of identification evidence are kept for a minimum period of five years after the relationship with the customer has ended unless the national laws and regulations provide for a longer period.

The date the relationship with the customer ends is the following date:

- a one-off transaction, or the last in a series of linked transactions, is carried out; or
- the business relationship ended, including the date of closing the account (accounts).

Records of all transactions reported to the Authorized body are kept for a minimum period of five years from the date of the transaction unless the national laws and regulations provide for a longer period.

Records of all internal and external reports are retained for a minimum of five years from the date the report was made unless the national laws and regulations provide for a longer period.

Besides, VTB Group Companies make and retain records of actions taken under the internal and external reporting requirements. When the AML Officer has considered information or other material concerning possible money laundering or terrorist financing, but has not made a report to the Authorized body, a record of the material that had been considered is kept as well.

TRAINING OF PERSONNEL

One of the most important controls over the prevention and detection of money laundering or terrorist financing is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of mandatory control transactions and unusual activities or transactions which may prove to be suspicious.

Therefore, VTB Group Companies relevant staff should be given appropriate training in order to be aware of:

- the legislation relating to money laundering and terrorist financing,
- the documents relating to the prevention of money laundering and terrorist financing issued by regulating and supervising authorities,
- the Company's policies and procedures of internal control in relation to the prevention of money laundering and terrorist financing,
- the potential effect on the whole VTB Group, VTB Group Company, its employees personally and on its customers, if any breach of the AML/CTF rules,
- their responsibilities in connection with the prevention of money laundering and terrorist financing, including those for obtaining sufficient evidence of identity, recognizing and reporting knowledge or suspicion of money laundering or terrorist financing, etc,
- the identity and responsibilities of the AML Officer.

It is recommended that VTB Group Companies' relevant staff and in particular employees engaged in customer acceptance, customer servicing, or in settlements receive training at least once a year. Following national laws and regulations, the circle of employees being trained may be broadened.

Extra trainings are given, if AML/CTF laws and regulations or the Company's policies and procedures in relation to the prevention of money laundering and terrorist financing have materially changed.

Relevant employees are trained in what they need to know in order to carry out their particular role. Staff involved in customer acceptance, in customer servicing, or in settlement functions need different training, tailored to their particular function. This may involve making them aware of the importance of the KYC requirements for money laundering prevention purposes, and of the respective importance of customer identification procedures, obtaining additional KYC information and monitoring customer activity.

The necessity of AML/CTF training is considered as well where staff moves between jobs, or change responsibilities.

CLOSING PROVISIONS

This Policy is subject to approval of the VTB Group Management Committee. After this Policy is approved by the VTB GMC VTB Group Companies shall use its provisions, which do not contradict with their national laws and regulations, for tailoring and improving their AML/CTF internal control rules.

This Policy is done in Russian and English. In case of divergent interpretation the Russian text shall prevail.

Appendix

Questionnaire / Вопросник

(to be filled by banks) / (заполняется банками)

I. Bank's Profile / Профиль банка

1.1.	Full registered legal name / Полное наименование	<input type="checkbox"/>	
1.2.	Short name / Краткое наименование	<input type="checkbox"/>	
1.3.	Legal form / Организационно-правовая форма	<input type="checkbox"/>	
1.4.	Registration number / Государственный регистрационный номер	<input type="checkbox"/>	
1.5.	Date of registration / Дата регистрации	<input type="checkbox"/>	
1.6.	Main state registration number (MSRN)* / Основной государственный регистрационный номер (ОГРН) <i>*For legal entities incorporated in the RF/ Для организаций, зарегистрированных в РФ</i>	<input type="checkbox"/>	
1.7.	Date of MSRN assignment / Дата присвоения ОГРН	<input type="checkbox"/>	
1.8.	Registration body / Орган государственной регистрации	<input type="checkbox"/>	
1.9.	Place of registration / Место регистрации	<input type="checkbox"/>	
1.10.	Tax identification number / ИНН (КИО)	<input type="checkbox"/>	
1.11.	Registered address / Адрес места нахождения (места регистрации)	<input type="checkbox"/>	
1.12.	Business address / Адрес фактического места нахождения	<input type="checkbox"/>	
1.13.	Correspondence address / Почтовый адрес	<input type="checkbox"/>	
1.14.	Telephone and fax numbers, e-mail / Номера телефонов, факсов, адрес электронной почты	<input type="checkbox"/>	
1.15.	Type of banking license / Вид лицензии на осуществление банковских операций	<input type="checkbox"/>	
1.16.	License number / Номер лицензии	<input type="checkbox"/>	
1.17.	Date of issue of the license / Дата выдачи лицензии	<input type="checkbox"/>	

1.18.	SWIFT, TELEX / СВИФТ, Телекс	<input type="checkbox"/>	
1.19.	Banking identification code / БИК	<input type="checkbox"/>	
1.20.	Registered and paid-in capital / Величина зарегистрированного и оплаченного уставного (складочного) капитала или уставного фонда, имущества	<input type="checkbox"/>	
1.21.	Codes of state statistics monitoring (if any) / Коды форм федерального государственного статистического наблюдения (ОКПО, ОКВЭД, ОКАТО, ОКОГУ)	<input type="checkbox"/>	

1.22. Please, provide information about your management bodies and mark those of them, which are present at your place of registration / Укажите, пожалуйста, сведения об органах управления Вашей организации и отметьте орган (органы), присутствующие по месту нахождения (месту государственной регистрации) Вашей организации:

1.22.1.	Management body / Орган управления	Surname, first name(s) / Фамилия, имя, отчество (если имеется)	Date of birth/Idата рождения
1.22.2.	General meeting / Общее собрание	<input type="checkbox"/>	
1.22.3.	Supervisory Council / Совет директоров (Наблюдательный Совет)	<input type="checkbox"/>	
1.22.4.	Chief executive officer (or equivalent) / Руководитель	<input type="checkbox"/>	
1.22.5.	Board of directors / Правление (дирекция)	<input type="checkbox"/>	
1.22.6.	Other persons authorized to act on behalf of your company / Иные лица, имеющие право действовать от имени Вашей организации без доверенности	<input type="checkbox"/>	

1.23. Please, provide information about your representative, who is authorised to enter into the agreement with us on behalf of your Bank / Укажите, пожалуйста, сведения о представителе кредитной организации, уполномоченном устанавливать договорные отношения:

1.23.1.	Surname, name(s) /Фамилия, имя, отчество (если имеется):	<input type="checkbox"/>	
1.23.2.	Date and place of birth / Дата и место рождения:	<input type="checkbox"/>	
1.23.3.	Nationality (citizenship) / Гражданство (подданство):	<input type="checkbox"/>	
1.23.4.	Residence address / Адрес места жительства (регистрации):	<input type="checkbox"/>	
1.23.5.	Contact address / Адрес места пребывания:	<input type="checkbox"/>	

1.23.6. Identity Paper (Passport or other document (specify), serial number, validity) / Сведения о документе, удостоверяющем личность (наименование, серия и номер, кем выдан (с указанием кода подразделения (если имеется)), дата выдачи, срок действия):

<input type="checkbox"/>	
<input type="checkbox"/>	

1.23.7. Position / Место работы и занимаемая должность:

<input type="checkbox"/>	
<input type="checkbox"/>	

1.23.8. Tax identification number (if any) / ИНН (при наличии):

<input type="checkbox"/>	
<input type="checkbox"/>	

1.23.9. Telephone and fax numbers, e-mail address / Телефон, факс, адрес электронной почты:

<input type="checkbox"/>	
<input type="checkbox"/>	

1.23.10 Migration card (number of the card, date of arrival and date of departure) / Миграционная карта (номер карты, дата начала и дата окончания пребывания) (for foreign citizens and stateless persons staying in Russia/ для иностранных граждан и лиц без гражданства, находящихся на территории РФ)

<input type="checkbox"/>	
<input type="checkbox"/>	

1.23.11. Visa, residence permit or other document permitting to stay (reside) in the Russian Federation (serial (if any) and number of the document, the date of commencement and the date of expiry of permission to stay in Russia) / Документ, подтверждающий право на пребывание (проживание) в РФ (серия (если имеется) и номер документа, дата начала и дата окончания срока действия права пребывания (проживания)) (for foreign citizens and stateless persons /для иностранных граждан и лиц без гражданства, находящихся на территории РФ)

<input type="checkbox"/>	
<input type="checkbox"/>	

1.24. Please, provide information about the persons, who are authorized to dispose of funds on your accounts / Укажите, пожалуйста, сведения о лицах, имеющих право распоряжаться денежными средствами на счёте (во вкладе) Вашей организации:

1.24.1. Surname, name(s) / Фамилия, имя, отчество (если имеется):

<input type="checkbox"/>	
<input type="checkbox"/>	

1.24.2. Date and place of birth / Дата и место рождения:

<input type="checkbox"/>	
<input type="checkbox"/>	

1.24.3. Nationality (citizenship)/ Гражданство (подданство):

<input type="checkbox"/>	
<input type="checkbox"/>	

1.24.4. Residence address / Адрес места жительства (регистрации):	<input type="checkbox"/>
1.24.5. Contact address / Адрес места пребывания:	<input type="checkbox"/>
1.24.6. Identity Paper (Passport or other document (specify), serial number, validity)/ Сведения о документе, удостоверяющем личность (наименование, серия и номер, кем выдан (с указанием кода подразделения (если имеется)), дата выдачи, срок действия):	<input type="checkbox"/>
1.24.7. Position / Место работы и занимаемая должность:	<input type="checkbox"/>
1.24.8. Tax identification number (if any)/ ИНН (при наличии):	<input type="checkbox"/>
1.24.9. Telephone and fax numbers, e-mail address / Телефон, факс, адрес электронной почты:	<input type="checkbox"/>
1.24.10. <i>Migration card (number of the card, date of arrival and date of departure)/ Миграционная карта (номер карты, дата начала и дата окончания пребывания)</i> (for foreign citizens and stateless persons staying in Russia / для иностранных граждан и лиц без гражданства, находящихся на территории РФ)	<input type="checkbox"/>
1.24.11. <i>Visa, residence permit or other document permitting to stay (reside) in the Russian Federation (serial (if any) and number of the document, the date of commencement and the date of expiry of permission to stay in Russia)/ Документ, подтверждающий право на пребывание (проживание) в РФ (серия (если имеется) и номер документа, дата начала и дата окончания срока действия права пребывания (проживания))</i> (for foreign citizens and stateless persons / для иностранных граждан и лиц без гражданства, находящихся на территории РФ)	<input type="checkbox"/>

1.25. Please, provide information about shareholders and beneficial owners holding 10% or more / Укажите, пожалуйста, сведения об акционерах (участниках) и бенефициарных владельцах, владеющих акциями (долями участия) в размере 10% и более.

	Name of shareholder and percentage of shareholding (%) / Наименование акционера (участника) и его доля в капитале (%)	Tax identification number and place of incorporation (residence), full address / ИНН (КИО) и адрес места нахождения	Main type of activity / Основной вид деятельности и	Name, date and place of birth of beneficial owner, % of shareholding / ФИО, дата и место рождения бенефициарного владельца, доля участия (%)	Residence address and main type of activity of shareholding / Адрес места жительства и род занятий бенефициарного владельца
1.25.1.					
1.25.2.					
1.25.3.					
1.25.4.					
1.25.5.					
1.25.6.					

1.26. Which institutions are your major correspondents and counterparts? / Укажите, пожалуйста, Ваших основных корреспондентов и контрагентов

	Name of company / Наименование	Place of incorporation (country, city) / Место нахождения (страна, город)
1.26.1		
1.26.2		
1.26.3.		
1.26.4.		
1.26.5.		

1.27. Do your services include e-banking and/or Internet-banking? / Использует ли Ваш банк электронные и/или Интернет - технологии при предоставлении своих услуг?

Yes / Да

No / Нет

1.28. Do you have a physical presence by way of real address and management bodies in the country of registration? / Имеет ли Ваш банк постоянный адрес и органы управления в государстве регистрации?

Yes / Да

No / Нет

1.29. Is your Bank a branch or a subsidiary of another institution? / Является ли Ваша кредитная организация филиалом, дочерним или зависимым обществом?

Yes / Да

No / Нет

1.29.1. Is your institution a branch of a bank? / Являетесь ли вы филиалом кредитной организации?

Yes / Да

No / Нет

1.29.2. If yes, please, give the name and address of the head (parent) company / Если да, назовите, пожалуйста, головную организацию и укажите адрес её места нахождения (регистрации).

--

1.30. Does your Bank have branches, subsidiaries, affiliates and representative offices? / Имеет ли Ваша кредитная организация филиалы и представительства, дочерние и зависимые общества?

Yes / Да

No / Нет

If yes, specify them / Если да, укажите их:

	Name of the company and its main type of activities / Наименование и основной вид деятельности	Place of incorporation (full address) / Место нахождения (регистрации) (полный адрес)	Surname, name(s) of CEO / ФИО руководителя	Banks, where accounts are opened / Обслуживающие банки
1.30.1.				
1.30.2.				
1.30.3.				
1.30.4.				
1.30.5.				

1.31. Please, describe (in general) your Bank's history, business reputation and market share / Опишите (в общем) историю Вашей организации, деловую репутацию и сектор рынка:

--

II. AML/CTF Controls / Противодействие легализации доходов, полученных преступным путём, и финансированию терроризма.

2.1. Are banks in your home country subject to laws tailored to counter money laundering and terrorism finance? / Являются ли банки в Вашей стране субъектами исполнения законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма?

Yes / Да

No / Нет

2.1.1. If yes, please, outline laws, rules and standards tailored in your country to prevent money laundering and terrorism financing / Если да, то укажите, пожалуйста, законодательные и иные нормативные акты в области ПОД/ФТ, принятые в Вашей стране:

2.2. Is your Bank subject to supervision for its anti-money laundering and terrorist financing practices by a State Supervisory/Regulatory Authority? / Осуществляет ли какой-либо государственный надзорный/регулирующий орган надзор за применением Вашим банком требований в области ПОД/ФТ?

Yes / Да

No / Нет

2.2.1. If yes, please state full name and address of your Supervisory/Regulatory Authority / Если да, пожалуйста, укажите полное наименование и адрес Вашего надзорного/регулирующего органа:

--

2.3. Has your Bank established internal policies, procedures and controls to ensure compliance with the obligations under the existing national legislation and regulations on prevention of money laundering and terrorism financing? / Разработаны ли в Вашем банке правила внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма и программы его осуществления в соответствии с требованиями национальных законодательных и иных нормативных актов?

Yes / Да

No / Нет

If yes, please, outline them / Если да, укажите их, пожалуйста:

	Title of internal AML/CTF act / Наименование нормативного акта	Date of last approval by supervisory authority (if provided by national legislation) / Дата последнего согласования с надзорным органом (если предусмотрено национальным законодательством)	Supervisory authority / Наименование надзорного органа
2.3.1.			
2.3.2.			

2.4. Has your Bank established the following procedures? / Разработаны ли в Вашем банке следующие процедуры?

2.4.1.	“Know Your Customer” procedures including customer and beneficiaries identification procedures / Идентификации клиентов, установления и идентификации выгодоприобретателей, изучения клиентов и контрагентов Банка.	<input type="checkbox"/> yes /да	<input type="checkbox"/> no / нет
--------	---	----------------------------------	-----------------------------------

Do your procedures include / Включают ли процедуры Вашего банка:			
2.4.2.	<input type="checkbox"/> Providing full details of the ordering customer (account number, name, full address) when fulfilling payment orders / Предоставление полных сведений о приказодателе (номер счета, имя/наименование, полный адрес) при выполнении переводов.	<input type="checkbox"/> yes / да	<input type="checkbox"/> no / нет
2.4.3.	<input type="checkbox"/> Identifying "walk-ins" (persons that do not have accounts with the bank) by passport/ID card when accepting cash payments and retaining a copy of this document in the bank / Идентификацию лица, не имеющего счёта в банке, при совершении им операции с наличными денежными средствами на основе его паспорта/другого документа, удостоверяющего личность, а также хранение копии этого документа в банке.	<input type="checkbox"/> yes, in all cases / да, во всех случаях <input type="checkbox"/> yes, if amount exceeds / да, если сумма превышает	<input type="checkbox"/> no / нет
2.4.4.	Checking information about the customers and their transactions / Проверки информации о клиентах Банка и совершаемых ими операциях	<input type="checkbox"/> yes / да	<input type="checkbox"/> no / нет
2.4.5.	Revealing transactions subject to AML/CTF legislation / Выявления операций, предусмотренных законодательством о ПОД/ФТ	<input type="checkbox"/> yes / да	<input type="checkbox"/> no / нет
2.4.6.	Documenting the revealed information and reporting transactions according to national AML/CTF legislation to the authorized body / Документального фиксирования и представления сведений, предусмотренных национальным законодательством о ПОД/ФТ, в уполномоченный орган	<input type="checkbox"/> yes / да	<input type="checkbox"/> no / нет
2.4.7.	Records keeping / Хранения документов и информации	<input type="checkbox"/> yes / да	<input type="checkbox"/> no / нет
2.4.8.	Confidentiality procedures / Обеспечения конфиденциальности информации	<input type="checkbox"/> yes / да	<input type="checkbox"/> no / нет
2.4.9.	Training of personnel in AML/CTF / Обучения персонала по вопросам ПОД/ФТ	<input type="checkbox"/> yes / да	<input type="checkbox"/> no / нет

2.5. Has your Bank developed standard forms to document information about customers? / Разработаны ли в Вашем банке анкеты клиентов?

Yes / Да

No / Нет

2.6. Do you have a risk focused assessment of your customers? / Оценивается ли в Вашем банке риск осуществления клиентами легализации (отмывания) доходов, полученных преступным путём, и финансирования терроризма?

Yes / Да

No / Нет

2.7. Do you determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the bank has reason to believe that they pose a heightened risk of illicit

activities at or through your Bank? / Определяет ли Ваш банк необходимые повышенные меры должной осмотрительности (due diligence) для соответствующих категорий клиентов и групп операций, которые, по мнению Вашего банка, связаны с повышенным риском проведения незаконных операций в Вашем банке или через Ваш банк?

Yes / Да

No / Нет

2.8. Does your Bank have policies covering relationships with Politically Exposed Persons? / Установлены ли у Вашего банка процедуры, регламентирующие отношения с иностранными публичными должностными лицами?

Yes / Да

No / Нет

2.9. Are your AML/CTF policies and practices applied to all branches and subsidiaries (if any) of your Bank both in the home country and in locations outside of the home country? / Применяются ли в филиалах и дочерних обществах Вашего банка (при их наличии) правила и программы внутреннего контроля в целях ПОД/ФТ, разработанные головной организацией банка?

Yes / Да

No / Нет

2.10. Is it AML Officer's duty to supervise the functioning of AML/CTF controls in all your branches (if any)? / Осуществляет ли Ответственный сотрудник по ПОД/ФТ Вашего банка контроль за организацией и функционированием системы ПОД/ФТ в филиалах Вашего банка (при их наличии)?

Yes / Да

No / Нет

2.11. Does your Bank open anonymous accounts to individuals and/or corporate customers? / Открывает ли Ваш банк счета на анонимных владельцев?

Yes / Да

No / Нет

2.12. Do you have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to operate in their countries of incorporation? / Разработаны ли в Вашем банке процедуры, должным образом обеспечивающие проведение операций только с теми банками-корреспондентами, которые обладают лицензиями на проведение банковских операций, выданными в странах их регистрации?

Yes / Да

No / Нет

2.13. Does your Bank have correspondent relationships with financial institutions residing in off-shore zones (off-shore zone meaning a country or a territory with preferential tax regime and/or legislation, which does not envisage disclosure of information on financial transactions)? / Поддерживает ли Ваш банк корреспондентские отношения с банками, зарегистрированными в государствах и на территориях, предоставляющих льготный налоговый режим и (или) не предусматривающих раскрытие и предоставление информации при проведении финансовых операций (оффшорных зонах)?

Yes / Да

No / Нет

If yes, please, name these correspondents / Если да, то укажите эти банки-корреспонденты:

2.13.1.	
2.13.2.	

2.13.3.

12.14. Does your Bank have “shell banks” as correspondents or counterparts? / Имеются ли в числе корреспондентов или контрагентов Вашего банка банки-нерезиденты, которые не имеют на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления?

 Yes / Да

 No / Нет

2.15. Does your Bank have correspondent relations with banks that open accounts to “shell banks”? / Имеет ли Ваш банк корреспондентские отношения с банками, в отношении которых имеется информация о том, что их счета используются банками, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления?

 Yes / Да

 No / Нет

2.16. Does your Bank collect information and assess the AML/CTF policies or practices of its own customers which are financial institutions? / Осуществляет ли Ваш банк сбор и анализ информации о правилах внутреннего контроля в целях ПОД/ФТ и практике их применения финансовыми учреждениями, являющимися клиентами Вашего банка?

 Yes / Да

 No / Нет

2.17. Do you have policies to communicate new AML related laws or changes to existing AML related policies or practices to relevant employees? / Существуют ли в Вашем банке процедуры доведения до сведения соответствующих работников информации об изменениях в законодательстве или процедурах внутреннего контроля в целях ПОД/ФТ?

 Yes / Да

 No / Нет

2.18. Does your Bank employ agents to carry out training functions? / Привлекает ли Ваш банк сторонние организации для обучения персонала?

 Yes / Да

 No / Нет

2.18.1. If yes, do you provide AML training to relevant agents that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving your Bank’s products and services and internal policies to prevent money laundering?/ Если да, то проводит ли Ваш банк обучение данных сторонних организаций на предмет выявления и направления сообщений об операциях, сведения о которых должны представляться в государственные органы, а также ознакомления с типовыми схемами отмывания преступных доходов с использованием продуктов и услуг Вашего банка, изучения правил внутреннего контроля в целях ПОД/ФТ?

 Yes / Да

 No / Нет

2.19. In addition to inspections by the government supervisors/regulators, does your Bank have an internal audit function or other independent third party that assesses the effectiveness of AML policies and practices on a regular basis? / В дополнение к проверкам, проводимым государственными надзорными/регулирующими органами, проводится ли в Вашем банке на регулярной основе оценка

эффективности правил и программ внутреннего контроля в целях ПОД/ФТ подразделением внутреннего контроля или внешним аудитором?

Yes / Да

No / Нет

2.20. Has your Bank been the subject of any investigation, indictment, conviction or civil enforcement action related to money laundering and terrorists financing in the past five years? / Применялись ли к Вашему банку меры воздействия надзорных органов в связи с неисполнением законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма за последние пять лет?

Yes / Да

No / Нет

If yes, please, provide more detailed information / Если да, то, пожалуйста, раскройте информацию подробно.

2.20.1.	
2.20.2.	
2.20.3.	

2.21. Does your Bank have Money Laundering Reporting Officer or another senior official designated to monitor suspicious client activities and to ensure compliance of your Bank with legislation and regulatory requirements relating to prevention of money laundering? / Назначен ли в Вашем банке сотрудник, ответственный за соблюдение правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма и программ его осуществления?

Yes / Да

No / Нет

If yes, please, provide his (her) full name, position, telephone and fax number & e-mail / Если да, укажите, пожалуйста его(её) фамилию, имя отчество (если имеется), должность, номера контактных телефонов и факсов, адрес электронной почты:

2.21.1. Full name / ФИО:	<input type="text"/>
2.21.2. Position / Должность:	<input type="text"/>
2.21.3. Telephone / Телефон:	<input type="text"/>
2.21.4. Fax / Факс:	<input type="text"/>
2.21.5. E-mail / Адрес электронной почты:	<input type="text"/>

On behalf of the bank / Уполномочен подписать от имени банка

(position / должность)	<input type="text"/>	<input type="text"/>
	(signature / подпись)	(surname, first name(s)/ ФИО)

Seal / Печать

Date / Дата