KSB COMMERCIAL BANK

"КСБ Коммерциялык Банк" ЖАК
КРУБ №020 лицензиясы
720005, Кыргыз Республикасы,
Бишкек ш., Байтик Баатыр көч., 68
тел.: +996 312 54 34 24
bank@ksbc.kg, www.ksbc.kg

ЗАО "Коммерческий Банк КСБ"
Лицензия НБКР №020
720005, Кыргызская Республика,
г. Бишкек, ул. Байтик Баатыра, 68
тел.: +996 312 54 34 24
bank@ksbc.kg, www.ksbc.kg

"KSB Commercial Bank" CJSC
NBKR licensed №020
68, Baitik Baatyr str., Bishkek
Kyrgyz Republic, 720005
tel.: +996 312 54 34 24
bank@ksbc.kg, www.ksbc.kg

Kyrgyz bank operating under laws and regulations of Kyrgyz Republic. Member of a Swiss Financial Group.

Letter
on Countering the Financing of Terrorist Activities and the Legalization (Laundering) of Proceeds of Crime

A compliance control system has been implemented and is operating at Closed Joint Stock Company "Commercial Bank KSB" (hereinafter referred to as the Bank). This system represents a set of organizational measures for internal monitoring, coordination, and control over compliance with and implementation of the requirements of the legislation of the Kyrgyz Republic in the field of combating the financing of criminal activities and the legalization (laundering) of proceeds of crime. The said system operates in accordance with the Law of the Kyrgyz Republic "On Combating the Financing of Criminal Activities and the Legalization (Laundering) of Criminal Proceeds" dated August 6, 2018 No. 87, as well as other regulatory legal acts of the Kyrgyz Republic in the field of CFT/AML.

The Bank has an independent structural unit - the Compliance Control Department - which ensures the implementation of legislative requirements in the field of combating the financing of criminal activities and the legalization (laundering) of proceeds of crime. For the purpose of complying with the said requirements of the legislation of the Kyrgyz Republic, the following internal regulatory documents have been developed and are applied:

- the Anti-Money Laundering and Counter-Terrorist Financing and Sanctions Compliance Policy of Closed Joint Stock Company "Commercial Bank KSB";
- the Internal Control Rules for the Purpose of Combating the Financing of Criminal Activities and the Legalization (Laundering) of Proceeds of Crime;
- the Anti-Corruption Policy of Closed Joint Stock Company "Commercial Bank KSB".

The set of measures implemented by the Bank within the AML/CFT framework includes, but is not limited to, the following:

- identification and verification of clients (the Bank does not open anonymous bank accounts or bearer accounts without client identification);
- assessment of client risks related to the possible legalization (laundering) of criminal proceeds and the financing of terrorist or extremist activities;
- identification and analysis of suspicious transactions, blocking of transactions involving persons included in the UN Security Council Consolidated Sanctions List, the Consolidated Sanctions List of the Kyrgyz Republic, as well as other international sanctions lists, including those of the European Union (EU), the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the UK HM Treasury (UK HMT), Canada, and other authorized international bodies;
- client due diligence procedures at the Bank are automated. The identification of suspicious transactions is carried out automatically through the Bank's automated banking system (ABS). Client screening is performed using the portal of the State Financial Intelligence Service under the Cabinet of Ministers of the Kyrgyz Republic (SFIS CMR), as well as other publicly available information sources.

The identification of sanctions and other risks is carried out using international resources LexisNexis Risk Solutions and Refinitiv. The use of the LexisNexis Risk Solutions platform enables the Bank to:

- automate and continuously perform screening of clients (both new and existing) and transactions (on a daily basis during non-business hours) against sanctions lists, including those of the UN Security Council, OFAC, the European Union (EU), HM Treasury (HMT), Rosfinmonitoring,

politically exposed persons (PEPs and related persons), as well as extended sanctions databases containing a significantly larger volume of information compared to official lists;
- identify payments to or from sanctioned persons, as well as transactions related to sanctioned territories (including specific localities), banks and their branches, offshore jurisdictions, and other restricted areas;
- automate the screening of international transactions and identify goods specified in payment documents that fall under sanctions or dual-use goods lists;
- minimize the number of false positives through the use of specialized LNRS extensions;
- generate and store reports and effectively manage false positive levels;
- apply LNRS extensions that allow identification of persons and entities in accordance with the "50%+ rule", including subsidiaries of sanctioned persons not explicitly listed in official sanctions lists of OFAC, the EU, HMT, and other regulators.

Authorized front-office employees of the Bank apply enhanced or simplified customer due diligence measures depending on the assigned risk level. Risk levels (high, medium, low) are determined based on the information and documents provided, taking into account the client's legal status, main business activity, geographic location, structure and volume of cash flows, nature of transactions, and other available information. Risk information is recorded in the client's questionnaire.

For clients with a high-risk level, the following enhanced measures are applied:

- collection of additional identification information and documents from reliable sources;
- obtaining extended information on the client and the beneficial owner to assess potential involvement in criminal activity;
- requesting information on the purpose and intended nature of the business relationship, as well as the source of funds;
- verification of sources of funds (the Bank does not accept documents in formats that allow copying or transferring signatures and seals);
- regular updating of information on the client and beneficial owner based on a risk-based approach;
- requesting additional explanations regarding the economic substance of transactions;
- obtaining approval from the Bank's executive body to establish or continue business relationships;
- enhanced transaction monitoring (including manual review), analysis of fund usage, and identification of suspicious indicators;
- monitoring using automated systems based on established threshold values;
- application of enhanced measures with respect to clients from high-risk countries.

For low-risk clients, simplified measures are applied:

- obtaining general information on the purpose of cooperation;
- verification of the client and beneficial owner after establishing business relations;
- reduced frequency of updating identification data;
- transaction monitoring using automated systems within established limits.

When assessing risks, the Bank considers the following risk categories:

- client risks: non-residents, companies with high cash turnover, complex ownership structures, bearer shares;
- geographic risks: countries with insufficient AML/CFT measures, countries subject to sanctions or embargoes, countries with high levels of corruption;
- product and delivery channel risks: private banking, anonymous transactions, receipt of funds from unknown third parties.

Clients classified as high-risk include:

- banks, casinos, offshore companies and banks, diplomatic missions, money transfer organizations, exchange offices, money remittance systems, check cashing points;

- virtual asset service providers and exchangers;
- dealers of vehicles, vessels, and aircraft;
- professional service providers (lawyers, accountants, investment brokers);
- travel agencies, brokers, and securities market dealers;
- traders of jewelry, precious stones, and metals;
- import-export companies;
- cash-intensive businesses (restaurants, retail outlets, parking services).

A high-risk level is assigned to a client in the presence of the following indicators:

- status as a religious, charitable, or other international non-profit organization;
- discrepancy between registered and actual addresses;
- presence of a politically exposed person (PEP) among beneficiaries or trustees;
- unusual or excessively complex ownership structure;
- existence of suspicious transactions;
- request from the Financial Intelligence Service for ongoing monitoring;
- daily transfers from one or more individuals to a legal entity (except for retail and catering businesses).

A high-risk level is also assigned in the following cases of account opening or transaction execution:

- remote identification;
- account opening based on a power of attorney;
- transactions uncharacteristic for the client, including those conducted via internet banking and electronic money.

In all other cases, the Bank is guided by the approved List of Suspicious Transactions.

The Bank does not establish correspondent relationships with non-resident banks that do not have a permanent management body in the country of registration, banks registered in offshore zones, or their affiliated or subsidiary entities if they are not independent legal entities. Additionally, the Bank does not cooperate with organizations registered in jurisdictions with preferential tax regimes and/or those that do not disclose information to regulatory authorities.

The Bank strictly complies with national legislation, regulatory requirements of supervisory authorities, and international AML/CFT standards, taking all necessary measures to minimize reputational, legal, and financial risks.

Sincerely,

Chairman of the Board **Chervonova K.V.**