Danske Bank Group Financial Crime Risk Statement for Correspondent Banking Relationships

Danske Bank Group A/S (Danske Bank) is committed towards combatting financial crime and complying with all applicable laws and regulations relating to financial crime to protect the Bank, its customers and its employees from financial crime related risks. Danske Bank has therefore adopted the following business policy (the Statement) towards its respondents in order to implement the highest standard of financial crime risk management practices, and to ensure full compliance with applicable anti financial crime laws and regulation.

1. KYC obligations

In order to fulfil Danske Bank's 'know your customer' (KYC) obligations, and in line with Section 13 of the General Conditions for Correspondent Banks[1], Danske Bank's relationship management and/or compliance teams may request information from you regarding your organisation and business, your direct customers, the transactions in your account(s) held with Danske Bank and the parties to those transactions, and any other information deemed relevant by Danske Bank in fulfilling its legal requirements. It is essential that you comply with such requests and provide complete responses within the specified timeframes.

2. Reporting obligations

Danske Bank requires you, to the extent legally permissible, to report any activity in your Danske Bank accounts that you have identified as illegal, illegitimate, unusual or suspicious. You should report this activity to your relevant Danske Bank Relationship Manager.

3. Prohibited transactions

Your Danske Bank accounts **must not** be used to conduct the following types of transactions (including transactions from any third parties that ultimately pass through your accounts held with Danske Bank) listed below:

- Transactions that breach applicable anti financial crime laws and regulations;
- Transactions that breach UN, EU, UK or US sanctions, or any other applicable sanctions;
- Transactions that relate directly or indirectly to Iran, North Korea, Cuba, Syria, Crimea, the Donetsk People's Republic and the Luhansk People's Republic[2];
- Transactions that appear to relate to any form of illegal activity including, but not limited to:
    - Illicit arms and munitions trafficking;
    - Illicit trafficking in narcotic drugs and psychotropic substances;
    - Illicit trafficking in stolen goods;
    - Illegal trade in conflict minerals and/or blood diamonds;
    - Illegal online gambling;
    - Organised crime and racketeering;
    - Terrorist activities, including terrorist financing;
    - Human trafficking and migrant smuggling;
    - Sexual exploitation; and
    - Any business that is known to be illegal in the jurisdiction in which the customer or business is resident, incorporated or operating.
- Transactions that involve shell banks or unregistered bearer share companies;

[1] https://danskeci.com/ci/relationship-banking/international-institutionals/nordic-clearing-services

[2] Plus any other countries which are included in the following lists:

- FATF's High-Risk Jurisdictions subject to a Call for Action
- Jurisdictions designated under section 311 of the USA Patriot Act
- Jurisdictions designated as State Sponsors of Terrorism by the US Department of State

- Transactions that facilitate tax fraud and tax evasion, and any aggressive tax arrangements or planning; and
- Transactions for or on behalf of underlying customers that are virtual currencies (cryptocurrencies) platforms / exchanges, or virtual currencies wallet providers
- Certain downstream correspondent banking transactions[3].

Danske Bank expects its respondents to maintain the appropriate transaction monitoring controls to ensure that Danske Bank accounts are not used for the types of transactions listed above. Where identified, Danske Bank may reject such transactions, issue cease and desist requests related to specific customers, and/or close your accounts with Danske Bank[4].

4. <u>Transactions involving higher risk industries</u>

Danske Bank considers certain industries to present a higher level of financial crime risk. As such, Danske Bank expects its respondents to maintain adequate internal policies and controls to ensure that transactions involving such higher risk industries do not violate applicable laws and regulations, and do not present an unacceptable level of financial crime risk. To the extent that the respondent's internal policies and controls are not capable of ensuring this, the respondent should not use its account(s) held with Danske Bank to process such transactions involving higher risk industries. The non-exhaustive list of industries considered as higher risk by Danske Bank is below:

- Arms, defence, military or atomic power industries
- Shipping, including cargo shipping
- Casino, lottery, gaming or other gambling-related services
- Crowdfunding businesses
- Dealers in precious metals, stones or jewels (or other high-value items)
- Extractive industries (e.g. mining, oil and gas)
- Marijuana related businesses
- MSBs (Money Service Businesses)
- MVTS (Money Value Transfer Services)
- NGOs (Non-Governmental Organisations)
- NPOs (Non-Profit Organisation)
- PSPs (Payment Service Providers)
- Red light business and adult entertainment businesses
- Virtual currencies platforms, exchanges, or wallet providers
- Unregulated charities

For transactions involving the higher risk industries listed above, Danske Bank reserves the right to request further information on the underlying business and parties involved, and/or to reject any such transactions in order to limit its financial crime risk.

Please take the necessary steps to ensure compliance with this Statement. Failure to comply with the requirements stated in this Statement may lead to rejection of transactions and/or closure of your account(s) with Danske Bank.

Should you have any questions regarding this Statement, please contact your relevant Relationship Manager.

---

[3] Danske Bank does not prohibit downstream correspondent banking transactions but such arrangements are subject to internal approval. Your Danske Bank Relationship Manager will inform you in instances where any downstream activity should be halted.

[4] As aligned with the agreed termination period in the cash agreement with the Respondent (if applicable)