BANQUE BANORIENT FRANCE LONDON - FINANCIAL CRIME COMPLIANCE STATEMENT

Background

We are the London Branch of Banque Banorient France Group with our head office in Paris. The Branch (the "Bank") was established in 1983 and for over 4 decades, have been serving Lebanese diaspora customers predominately based in the Levant, Gulf states and the U.K. We are regulated by both the Prudential Regulatory Authority and the Financial Conduct Authority in addition to our parent Bank's Regulator, the French ACPR.

Money laundering and terrorism finance are a major threat to the international financial services Industry. We are committed to robust standards in our Anti Money Laundering (AML) and Combating Financial Terrorism (CFT) frameworks which we review annually to ensure our controls remain up to date and effective in combating money laundering, terrorism finance, proliferation finance and tax evasion.

Legal and Regulatory Framework

Our Group AML and CFT policy and procedures are complemented by UK policy and procedures. We manage our money laundering and sanctions risks on a risk-based approach, considering both EU and UK money laundering regulations and our business model. We have adopted best practice and standards by guidance of the FCA, FATF, the JMLSG and the Wolfsberg Group. We also regularly review and adopt best practices recommended following findings in penalty notices issued by the FCA for AML failings as well as other recommendations issued by advisory bodies such as Action Fraud. We recognise that constant vigilance is key to preventing the proceeds of crime passing through our Bank and the financial markets.

The MLRO has oversight of the AML activities for the branch and is the nominated officer for reporting suspicious activities to law enforcement agencies. The business remains the owner of customer and product/services risks and ensure that the customers they onboard are within the Bank's risk appetite. We recognise that customer risk assessment is a dynamic process and thus we conduct regular reviews on KYC files and account operations. We will exit any customer relationship that no longer fit our risk appetite.

Policy and Procedures

Our Group AML & CFT policy and procedures provide framework for management of money laundering and sanctions risks across all the branches to prevent the use of the Bank's products and services to facilitate money laundering, terrorism finance and tax evasion. The Bank works with other banks, UK regulators, Government, and law enforcement agencies to achieve UK and international goals in reducing financial crime, terrorism and proliferation financing and human rights violation. Where interpretation of EU and UK regulations differ, we apply the more stringent of the regulations to our UK AML framework.

We only open accounts and do business with customers that we have been fully identified. Our onboarding and customer due diligence procedures are based on UK Money Laundering Regulations 2017, subsequent amendments and associated legislation such as The Companies Act 2006 which set out clearly the elements we must satisfy when we establish banking relationships. We therefore request information on the purpose of account, how the customer intends to operate it, source of funds and source of wealth. Where we identify higher risk customers such as Politically Exposed Persons (PEPs), we will always apply enhanced due diligence and seek senior management approval. The Bank is aware of the higher risks of bribery and corruption when dealing with PEP accounts and as such manages this customer category via a PEP register and enhanced monitoring.

All customers are risk assessed at onboarding stage and their risk score determines their KYC review cycle. In addition to the initial risk assessment, the Bank periodically reviews the risk rating for each customer as part of its KYC review cycle and ensures that it holds up to date information through customer engagement. At Banorient France London, we always attempt to meet new customers face to face. Although some customers are referred from our Group branch network, our risk assessment is independent and we will not proceed with account opening unless we are fully satisfied with our due diligence. We will reject any business that falls outside our risk appetite or that cannot satisfy our due diligence checks. There are certain business sectors such as casinos, arms manufacture/trade and diamond mining which we will not onboard. We also do not open accounts for firms trading in crypto-assets which is outside our risk appetite.

Sanctions

We will not transact with sanctioned countries, sanctioned individuals, entities and prohibited industries. To comply with UK and international sanctions, we screen all incoming and outgoing payments and will delay or freeze payments for further investigation to ensure we do not breach any sanctions.

Suspicious Activity Reporting

We will request further information on source of funds from remitters and pursue information until we receive satisfactory responses, otherwise we will report suspicion to the relevant law enforcement agencies. We will work with them and comply promptly with freezing orders served on us.

Record-keeping

We are data processor registered with the ICO and comply fully with the Data Protection Act 2018 and subsequent amendments which incorporate the EU GDPR provisions.

Customer records are kept for up to 7 years and this is reflected in our Privacy Notice made available to the customer at onboarding and published on our website. The Privacy Notice also explains how the Bank collates and uses customer data.

While the banking relationship is ongoing, we are required to keep customer files up to date to undertake our KYC review and transaction monitoring so we will contact customers from time to time for further information. We expect full co-operation to comply with our legal obligations in this aspect.

Staff Training

We believe that staff training is a vital tool to keeping their AML knowledge up to date and enhance their understanding of risks in their day to day work. All staff must complete and pass compulsory training in:

- Anti-money laundering
- Anti-Bribery and corruption
- Sanctions
- Data protection
- Code of Conduct
- Whistle-blowing

Frontline staff who interact with customers are reminded that they play a role in combating money laundering and terrorism finance risks and that if they have suspicion or knowledge, then they must report via our Bank's Suspicious Activity Reporting process.

Code of Conduct

All staff must also complete their annual compulsory training on the Bank's Code of Conduct. The Bank keeps a gift register and has clear procedures on corporate gifts and entertainment which apply to all staff. Staff are encouraged to speak out on conduct issues and to report any misconduct via the Bank's reporting process. The MLRO is the Bank's whistle-blowing champion.

Third Parties

Where third parties are involved in the provision of services to support our banking facilities to customers, we ensure they meet our stringent checks and adhere to our standards and values. The Bank operates a strict vetting process of our third parties and will not continue our contractual relationship with any party that breaches our standards and values.

Whistleblowing

All staff are made aware of the Banks Whistle Blowing Policy and assured that they are fully protected should they submit a Whistleblowing report or make a claim of potential wrongdoing.