THIRD PARTY PRIVACY NOTICE
The Bank of Nova Scotia, London Branch and Scotiabank Europe plc

The Bank of Nova Scotia, London Branch ("**BNS**") and Scotiabank Europe plc ("**SBE**") are committed to respecting individuals' privacy.

BNS is incorporated in Canada and is a chartered schedule I bank under the Bank Act (Canada). BNS's place of business in the United Kingdom is 201 Bishopsgate, 6th Floor, London, EC2M 3NS. SBE is incorporated in England and Wales under number 00817692. SBE's place of business in the United Kingdom is 201 Bishopsgate, 6th floor, London EC2M 3NS.

For the purposes of data protection law, BNS and SBE are each a data controller in respect of personal data that they process in connection with their business and the products and services that we provide. In this notice, references to "**we**", "**us**" or "**our**" are references to BNS and SBE.

1. About this privacy notice

As data controllers, we are responsible for ensuring that we use individuals' personal data in compliance with data protection law.

This privacy notice applies to the personal data we may gather in connection with the operation of our business and the products and services that we provide and sets out the basis on which we will process such personal data.

2. Personal data that we collect

We collect the following personal data about individuals:

- **Information that is provided by you directly or through your agent to us or one of our affiliates**. This includes information provided directly, whether by filling in forms, face-to-face, by phone, by letter, e-mail or otherwise. This information may include:

    - data collected whilst communicating with us, such as full name, gender, business or personal contact details (address, home and mobile telephone numbers), occupation, job position / title and area of responsibility, family details, marital status, location
    - data gathered for due diligence purposes, for example, identification documents, including passport, date of birth, photographs, age, citizenship, nationality, residency, government issued identifying numbers (passport / national insurance / social security numbers), source of wealth / funds
    - other information, including in relation to recruitment, such as data provided on CVs, work history, regulatory registrations and work eligibility

- **Information we collect or generate.** This includes information that we generate about staff at our customers or suppliers. This information may include:

    - interactions with our staff, captured in customer relationship management systems or in our email system (including but not limited to email address and the content, date and time of interactions / correspondence) or in telephone and mobile communications (including call recordings)

- CCTV images and access records in respect of visitors to our office
- information provided on application forms

- **Information we obtain from other sources**. This includes information that we obtain in connection with "know your customer" ("**KYC**") and anti-money laundering checks ("**AML**"), and information provided to us by an individual's employer in connection with our business relationship with the employer or for recruitment purposes. This information may include:

    - data collected via searches on publicly available sources, for example sanctions and media / internet searches, criminal background checks and status as a politically exposed person or connection to politically exposed persons
    - data collected via a third party source (such as from an individual's employer, recruitment agencies or screening tools), including copies of identity documents (as detailed above)

3. Uses of personal data

Personal data may be stored and processed by us and / or affiliates for the following purposes:

- to enable us to provide a range of products and services to our customers on an ongoing basis

- for our legitimate interests, including:

    - to market our products and services to customers and potential customers appropriately
    - to maintain our relationships with customers and for marketing or business development purposes
    - to receive services from suppliers and manage and monitor our relationship with suppliers
    - to effectively and efficiently administer and manage the operation of our business, for example in respect of recruitment, investigating complaints and for risk management purposes
    - to undertake security and compliance monitoring, including of communications, to detect, investigate and resolve information, cyber and other security threats, compliance with policies, procedures and / or applicable law and regulation
    - to maintain our own books and records

- to comply with legal and regulatory requirements, including record keeping, undertaking conflicts checks, reporting (including trade and transaction reporting) and responding to regulatory investigations and requests

- to prevent and detect financial crime

- to establish, exercise or defend our legal rights or for the purpose of legal proceedings

4. Legal basis for using personal data

We will only process personal data where there is a legal basis to do so. We are entitled to use personal data as outlined in this notice because:

- we need to provide our products and services to our customers in accordance with our terms of business or other contracts with customers; if we are not provided with this information, we will not be able to carry out the relevant contract

- we have legal and regulatory obligations that we have to discharge

- we may need to in order to establish, exercise or defend our legal rights or for the purpose of legal proceedings

- its use is in accordance with our legitimate interests (or the legitimate interests of one or more of our affiliates), as outlined in this notice under “Uses of personal data” above.

- where applicable, individuals have consented or explicitly consented to the using of their data in a specific way

5. Disclosure of personal data to third parties

We may disclose personal data to our affiliates for the purposes of:

- the management and administration of our business and our affiliates’ business

- ensuring and monitoring compliance with legal and regulatory obligations, for example trade and transaction reporting obligations, market abuse monitoring, KYC / AML monitoring and internal policies and procedures

We take steps to ensure that the personal data is accessed only by employees of such affiliates that have a need to do so for the purposes described in this notice.

- We may also share personal data with third parties (including service providers, professional advisors and contractors), enforcement / fraud prevention agencies, trading venues and regulators. This may include the following:

- information provided to service providers (for example IT and communications advisers, providers of our electronic data storage services), professional advisors (for example law firms, accountants and auditors) or contractors for the purposes of providing services to us

- information provided to trading venues, enforcement / fraud prevention agencies and regulators to fulfil our legal and regulatory obligations, including in relation to trade and transaction reporting, investigations and financial crime reporting

- in the event we sell any of our business or assets or are acquired, we may disclose personal data to the buyer if necessary, including for due diligence purposes

Third parties will be subject to appropriate data protection and confidentiality requirements under the terms of their contract with us. Trading venues and regulators will maintain their own privacy notices as controllers which can be viewed on the relevant websites.

We may also disclose personal data to the extent required by law, regulation or court order or to establish, exercise or defend our legal rights.

6. Transfers of personal data outside the European Economic Area

The personal data that we collect may be transferred to, and stored at, a destination outside the European Economic Area (“**EEA**”). It may also be processed by individuals operating outside of the EEA who work for our affiliates or for one of the third parties described above.

Where we transfer personal data outside the EEA, we will ensure that it is protected in a manner that is consistent with how personal data will be protected by us in the EEA. This can be done in a number of ways, for instance:

- the country that we send the data to might be approved by the European Commission as offering a sufficient level of protection
- the recipient might have signed up to a contract based on "model contractual clauses" approved by the European Commission, obliging them to protect personal data
- the recipient may be party to binding corporate rules (relevant to intra-group transfers only)
- where the recipient is located in the US, it might be a certified member of the EU-US Privacy Shield scheme

In other circumstances the law may permit us to otherwise transfer personal data outside the EEA. In all cases, however, we must ensure that any transfer of personal data is compliant with data protection law.

Individuals can obtain more details of the protection given to their personal data when it is transferred outside the EEA (including a copy of the standard data protection clauses which we have entered into with recipients of their personal data) by contacting us in accordance with the "Contacting us" section below.

7. Retention of personal data

We will store personal data on necessary databases and personnel files that may include both soft and hard copy form. How long we hold personal data for will vary. The retention period will be determined by various criteria including:

- the purpose for which we are using it – we will need to keep the data for as long as is necessary for that purpose
- legal obligations – laws or regulation may set a minimum period for which we have to keep personal data

Retention periods may be extended if we are required to preserve personal data in connection with legal proceedings. Upon request, we can provide more information on retention periods related to individuals' personal data.

8. Individuals' rights

Individuals have a number of legal rights in relation to the personal data that we hold. These rights include:

- the right to obtain information regarding the processing of personal data by us, and a copy of the personal data which we hold
- where individuals have actively provided their consent for us to process personal data, the right to withdraw consent at any time. Please note that we may still be entitled to process personal data if we have another legitimate reason (other than consent) for doing so
- the right to request that we rectify personal data if it is inaccurate or incomplete

- the right to request that we erase personal data in certain circumstances. Please note that there may be circumstances where we may be asked to erase personal data but we are legally entitled to retain it

- the right to object to, and the right to request that we restrict, our processing of personal data in certain circumstances. Please note that may be circumstances where we are legally entitled to continue processing personal data and / or to refuse such requests

- the right to lodge a complaint with the data protection regulator (details of which are provided below) if individuals think that any of their rights have been infringed by us

Individuals can exercise their rights by using the details set out in the "Contacting us" section below and can find out more information about their rights by contacting the Information Commissioner's Office (https://ico.org.uk/).

9. Protection of personal data

We have implemented appropriate technical and organisational measures to protect personal data, which are required whether personal data is held electronically or in paper form and whether it is at rest or in transit. Technical measures, for example, include using encryption tools to protect data held in electronic form or pseudonymisation, where appropriate. Organisational measures, for example, include storing paper records containing personal data in locked cabinets and / or restricted areas.

10. Contacting us

Individuals who would like further information about the processing of their personal data, to make a related complaint or to exercise any of the rights listed above, should contact the Compliance Department, The Bank of Nova Scotia / Scotiabank Europe plc, 201 Bishopsgate, 6th Floor, London, EC2M 3NS; Fax Number: +44 (0)20 7826 5960; Email: LONDataProtection@scotiabank.com.

Where applicable, individuals may be required to supply a valid means of identification as a security precaution to assist us in preventing the unauthorised disclosure of personal data.

11. Changes

The content of this privacy notice may change from time to time and updated versions will be made available, including on our website (http://www.gbm.scotiabank.com/AboutUs/AB_Global_Presence.htm).