



Standard Bank
Offshore

STANDARD BANK OFFSHORE

STAFF PRIVACY STATEMENT

Effective 01 January 2025

Standard Bank Offshore

STAFF PRIVACY STATEMENT

Effective 01 January 2025



What this Privacy Statement covers and contact details

This Privacy Statement applies to all staff (as defined below) (“you, your”) of any company (a data controller) within the Standard Bank Offshore Group (“we, us, our”).

“Standard Bank Offshore Group” is the collective term for a group of companies that are based in Jersey, the Isle of Man and Mauritius, and which are ultimately jointly owned by Standard Bank Group Limited and Standard Bank Group International Limited. Details of the companies that comprise the Standard Bank Offshore Group and their contact details can be found at the end of this statement.

The relevant Standard Bank Offshore Group data controller(s) in respect to your personal information will, unless otherwise stated, always be the Standard Bank Offshore Group company(ies) with whom you:

- a) have made a work-related enquiry to but have not yet formally applied to; and/or
- b) are presently applying to for work and/or to provide your services to or for the benefit of; and/or
- c) already have a formal written contract with (either a contract of employment or a contract for services, a letter of engagement, and/or terms and conditions, and/or a written agreement, and/or any other legally binding documentation) for you to work for and/or provide your services to or for the benefit of; or
- d) do not yourself have a formal written contract directly with but you are associated or connected (for example, as an employee or consultant), to a consultancy business or other business concerned with the supply of services to that Standard Bank Offshore Group company(ies), and in the course of such association or connection you work for and/or provide your services to or for the benefit of a Standard Bank Offshore Group company in such a way that Standard Bank Offshore Group company comes to obtain and/or process your personal information, then the Standard Bank Offshore Group data controller(s) in respect to your personal information will be the Standard Bank Offshore Group company(ies) that business has either enquired of, and/or applied to, and/or has a formal written contract with (either a contract of employment or a contract for services, a letter of engagement, and/or terms and conditions, and/or a written agreement, and/or any other legally binding documentation) for it to work for and/or provide its services to or for the benefit of.

For the purposes of this Privacy Statement “staff” is to be given its widest possible interpretation and includes, but is not limited to, any natural person being a past, present or prospective employee (with a contract of employment) or consultant (with a contract for services or working pursuant to such a contract with a consultancy practice) with a Standard Bank Offshore Group company or companies, regardless of where situated and whether undertaking voluntary or paid work. Staff also includes any past, present or prospective person on secondment or work experience or as part of an internship programme with a Standard Bank Offshore Group company or companies and regardless of whether these arrangements are undertaken voluntarily or are paid.



Standard Bank
Offshore



The Standard Bank Offshore Group's appointed representative in the European Union for data protection purposes can be contacted at:
EURepresentative@standardbank.com

The Standard Bank Offshore Group's appointed Data Protection Officer ("DPO") can be contacted on the below details:

Jersey:

Data Protection Officer
Standard Bank Jersey Limited 47–49 La Motte Street
St. Helier Jersey JE2 4SZ
Email: dpo@standardbank.com

Isle of Man:

Data Protection Officer
Standard Bank Isle of Man Limited One Circular Road
Douglas Isle of Man IM1 1SB
Email: dpo@standardbank.com

Mauritius:

Data Protection Officer
Standard Bank Trust Company Mauritius Limited Level 10, Tower A
1 CyberCity Ebene Mauritius
Email: dpo@standardbank.com

Standard Bank Offshore Group Human Capital ("SBOGHC") is a division of both Standard Bank Isle of Man Limited and Standard Bank Jersey Limited but is effectively a shared resource for the wider Standard Bank Offshore Group for whom it processes the personal information of all staff.

Regardless of which Standard Bank Offshore Group company(ies) is/are your data controller(s) we treat the personal information we collect from you or about you through, for example, any application forms you may complete (electronically or in hardcopy), our website(s), associated websites, mobile sites, mobile applications and other communication channels as private and confidential.



This Privacy Statement provides an overview of:

- the type of personal information we collect and use;
- the purposes for which we use it (including whether you have an obligation to provide us with your personal information and any consequences of you not doing so);
- how we collect your personal information;
- where we keep your personal information;
- how we keep your personal information secure;
- who we disclose your personal information to and where those recipients are in countries outside of those of the Standard Bank Offshore Group how we safeguard those arrangements;
- how long we keep your personal information for;
- your rights in respect to your personal information and how you can exercise those rights; and
- whether your personal information is subjected to any automated decision- making, including profiling, and information about the logic, the significance and envisaged consequences of that decision making for you.



What is personal information, and what personal information do we collect, have or compile about you?

Personal information is information which identifies an individual person or from which an individual person is identifiable.

Depending on the nature and means of your enquiry and/or the work/services you provide to or for our benefit then we will typically collect and use:

- your contact information: your name (and any previous names); your home and/or business address(es); your telephone number(s); and email address(es);
- other personal information about you: your identity and/or passport documentation; proof of address documentation; your bank account and tax status and information; salary and benefits details; your residential and work permit status; your marital status; your gender; date and place of birth; your present and previous occupations and employers; employment start and finish dates; business unit and job title; staff number; your qualifications and educational history (including institutions attended); your professional and personal referees and references; your emergency contact/next of kin contact details; criminal convictions, professional misconduct and credit check information; your psychometric test results (if relevant); your photograph; information relating to your hobbies/achievements outside of work and that you may provide to us; interests or club/charity memberships/involvements; information on training and qualification courses you have undertaken or to be undertaken; your personal goals, objectives and development plans; personal performance information for appraisal/disciplinary purposes (which will include both factual and opinion information, of both you and other staff members, regarding you); your expense claims, travel claims, pension contributions and details and, if applicable, time sheets; flexible working arrangements; your holiday entitlement and days off or to be taken off; and information on your investment dealing activities;
- personal information about you that is collected in the context of our monitoring activities: facilities access and user information within our offices captured via our secure swipe card/app, office and floor entry systems and our printer/scanner access control system; CCTV footage taken in/on our premises; recorded telephone conversations to which you are party; and website and email usage while you are utilising Standard Bank's IT systems;



- certain “special category/sensitive personal information”: information relating to your physical, mental and occupational health (as it is relevant to sick leave, allergies or other medical conditions which may affect your employment or the benefits we provide) and disability related information; ethnicity; religion; sexual orientation.
- personal information about your dependent family members: their names; dates of birth and health related details if relevant for medical aid or benefit purposes; their financial interests if relevant for auditor independence purposes as well as for outside business interest declarations – where this is the case please bring this privacy notice to their attention; and
- personal information relating to business assets: your computer serial number; password/user authentication information; telephone line; workstation detail; and desk number; and
- certain other personal information about you as collected by our cookies when you visit our web pages (see further explanation below and the cookies pop-up we use when you visit our applicable websites).

The personal information mentioned above is an indicative list only and not exhaustive.



Why we use your personal information?

As staff of a Standard Bank Offshore Group company we collect, use and share your personal information primarily:

1. to ensure we comply with any applicable employment or other relevant laws (for example, disability discrimination, equal opportunities, health and safety legislation) that we are subject to as regards our engaging you; and/or
2. where you are enquiring or applying to become, or already are one of our existing staff members and would have/do have a contract directly with us, then as is necessary for the performance of, or to take steps on your behalf and at your request to enter you into, that contract that you are, or will be, party to with a relevant Standard Bank Offshore Group company as staff.

We therefore will need to gather and use your personal information for staff administration/employment purposes during our recruitment and selection processes, our verification and pre-employment vetting checks, the period in which you work for/with us, and as a result of our monitoring activities.

Where we collect and use and share your personal information on the above legal bases then failing to provide the necessary personal information to us will impact our ability to offer you a position with us and/or our ability to continue offering you a position with us and/or our ability to pay you, accommodate your work related requirements, and/or provide benefits to which you may otherwise be entitled.

Where our collecting and use of your personal information is not necessary pursuant to a contract that you have/would have directly with us nor to ensure we comply with any particular legal obligation then we will only collect and process your personal information:

1. if it is in your or a third party's vital interests for us to do so (for example, in an emergency situation where harm may otherwise result); or
2. in circumstances where:
 - a) the personal information is not sensitive/special category information; and
 - b) we or a third party have a legitimate interest in using it; and
 - c) after considering your personal fundamental rights and freedoms, we do not determine that legitimate interest is, on balance, overridden by those rights and freedoms; and
 - d) in undertaking that balancing exercise we have taken into consideration your reasonable expectations as to what the information might be used for based upon your relationship with us.

We presently rely on this legitimate interests basis to use and share your personal information for:

- i) communication purposes;
- ii) prevention and detection of crime;
- iii) salary and benefit provision and delivery;



- iv) business intelligence management information generation;
- v) strategic and organisational planning and management of our workforce generally;
- vi) IT support services;
- vii) the safety of our clients, staff and the wider public;
- viii) internal administrative purposes;
- ix) for handling enquiries, complaints and legal claims; and
- x) training and monitoring purposes.

Where we are not required to share your personal data with a 3rd party by law, or because such sharing is necessary pursuant to a contract to which you are party or to take steps at your request to enter you into such a contract, then we also rely on it being in our legitimate interests for the above purposes to share your personal information with:

- i) the wider Standard Bank Group of companies (see <http://www.standardbank.com/pages/StandardBankGroup/web/docs/Oursubs2017.pdf> for our different Standard Bank offices and their locations); and
- ii) any recruitment agency/business/professional services business that you have been using to liaise with us; and
- iii) other trusted third parties that we work with to accommodate your working arrangements, provide you with benefits, support our business.

For more specific information on who we share your personal information with please see "Who we disclose your personal information to and why".

- 3. in very rare cases, where the personal information is special category/ sensitive information and our using it is necessary to exercise, bring or defend a legal claim.

In some limited circumstances, we may also seek your explicit consent to our collecting and/or using and/or sharing your personal information. Where this is the case then we will fully inform you of what we plan on doing with the information and you will then be asked to confirm your consent to our using this information in the manner proposed and have the right to withdraw that consent at any time.



Our use of technology to follow your use of our websites

While you are making use of our websites, mobile applications, we automatically process certain information such as information about visits to our website. We use this information to find out which areas of our website people visit most and to monitor usage of our websites. This helps us to add more value to our services. This information is gathered in such a way that we do not get personal information about any individual or their online behaviour on other websites. Although it is possible to identify visitors to this website using internet provider addresses we do not do so except in cases of fraud or attempted fraud. To protect against fraud we undertake a number of security checks. The information we collect may be supplemented with information from third party sources. The information gathered is used solely by the Standard Bank Offshore Group and shall not be disclosed to any other person unless under compulsion of law or to protect Standard Bank Offshore Group's legitimate interests.

Cookies

As you may already be aware from our website cookie pop-up messages, we use cookie technology on some of our websites. A cookie is a small text file that is saved on your Internet browser when you use our websites. The cookie is sent to our computer each time you visit our websites. Cookies make it easier for us to give you a better experience online. You can stop your browser from accepting cookies, but if you do, some parts of our websites or online services may not work. We recommend that you allow cookies.



Links to other websites

Our website, related websites and mobile applications may have links to or from other websites. Although we try to link only to websites that also have high privacy standards, we are not responsible for their security, privacy practices or content. We recommend that you always read the privacy and security statements on these websites.

Monitoring and/or recording of communications and other activities

We communicate with you and with our clients through different methods and channels and we always endeavour to facilitate and support your working practices by providing comfortable and safe environments in which to work and IT hardware, software and systems for business purposes.

Where required by law or where we have considered it to be in our legitimate interests for the prevention and detection of crime, the safety of our clients, staff and the wider public, for handling enquiries, complaints and legal claims, or for training and monitoring purposes, we also record and/or monitor:

- i) emails to and from your Standard Bank email address;
- ii) websites that you visit using our IT equipment and systems;
- iii) telephone conversations to and from your Standard Bank telephone;
- iv) your building/floor secure access and printer/scanner facilities usage; and
- v) your CCTV image when you are in one of our CCTV covered areas.

Social media

We operate and communicate updates through our designated channels, pages and accounts on some social media sites to inform, help and engage with our customers. We monitor and record comments and posts made about us on these channels so that we can improve our services.

The general public can access and read any information posted on these sites.

We are not responsible for any information posted on those sites other than the information posted by our designated officials. We do not endorse the social media sites themselves, or any information posted on them by third parties or other users.

When you engage with us through social media your personal information may be processed by the site owner; this process is outside our control and may be in a country outside of the Isle of Man, Jersey and Mauritius that may have different privacy principles.

Social media sites are not appropriate forums to discuss our customers' products or financial arrangements. We will not ask you to share personal, account or security information on social media sites.

We regularly update and monitor our social media accounts and welcome feedback and ideas sent to us through these channels. We try to join conversations whenever possible, but may not reply to all messages sent to official Standard Bank social media accounts.



How do we obtain your personal information?

Most of the personal information we have about you is or was provided either:

- i) directly from you; or
- ii) any recruitment agent/business you liaised with us through;
- iii) or any consultancy business or other business concerned with the supply of services to a Standard Bank Offshore Group company(ies) with which you are associated/connected;
- iv) during our recruitment and on-boarding process or during the course of your working for/with us.

Your role in Standard Bank Offshore Group requires honesty and integrity in all of your dealings. To help us to determine this then in addition to personal information obtained from the above sources we also ask you to provide us with referees we may contact to obtain references from on your behalf, liaise with third parties to undertake risk,



integrity, regulatory and related background screening and verification checks and in some cases psychometric testing.

The extent of the background/verification checks we undertake and the information obtained as a result varies depending on:

- i) the seniority and nature of the position/services you are to fill/provide for us; and
- ii) your previous employment and education/qualifications/professional body memberships; and
- iii) by country/territory to comply with local requirements;

but it may also include information we gather from publicly available sources, and where lawful and reasonable, from other sources such as your former employers or colleagues, schools you have attended, academic qualification registers, credit reporting agencies and criminal records databases. You will receive information about the nature of such a background check before it begins.

Other personal information about you is compiled on an on-going basis during the course of your employment/provision of services to us as a result of:

- i) our monitoring certain of your activities (please see “Monitoring and/or recording of communications and other activities” section above as to what personal information we obtain when we undertake those activities); and
- ii) as part of the annual goal setting and performance appraisal process in which you take part, and/or any grievance and/or disciplinary proceedings you may be involved in; and
- iii) general staff administration (attending to leave, expenses, and other working arrangements).



Where we keep your personal information

Most of the personal information about staff is held by SBOGHC and can be viewed and accessed by employees via the Human Capital management system or your applicant profile created in the Careers Portal, as the case may be.

Employees are encouraged to regularly check and update the personal information SBOGHC has on record through the approved mechanisms. In situations where information cannot be viewed and updated by yourself, you should request assistance from the relevant SBOGHC representative assigned to your business area.

Other electronic systems and databases are also used to process your personal information for the purposes of administering staff related activities. All such systems and databases only collect, receive, use and share your personal information in accordance with, and as permitted by applicable laws, or internal business policies, standards and processes applicable to Standard Bank Offshore Group.

Where staff personal information is retained in hard copy (paper) format it is kept secure and safe in locked secure storage.



How we keep your personal information secure

We use appropriate technical and organisational measures to keep your personal information secure taking into account, amongst other things, the sensitivity of the personal information, the number of staff whose personal information we collect and process, the technologies available to secure it and their cost.

These measures are specifically designed and updated to prevent unauthorised access to/processing of your personal information and/or its accidental loss, destruction or damage. A general description of some of these security measures are set out below.

All our Standard Bank Offshore Group offices are equipped with certain physical access/security systems including secure entry systems and auto-lock door mechanisms, alarm and CCTV systems.

All staff within those offices are subject to our standard take on and vetting processes and have contracts obliging them to keep our information confidential and restricting their use of that information.

All staff are further obliged to adhere to comprehensive written policies and procedures and undertake regular and ongoing training. These address, amongst other things, our clear desk policies, screen locking, use of own devices, disposal of confidential waste, encryption of data, and the use of passwords on the systems they use. Certain staff also have assigned roles and responsibilities to help ensure the security and integrity of our information – including our Data Protection Officer. We restrict access to our IT systems to those personnel that require it in the performance of their role(s) and where possible endeavour to anonymise the personal information held.

Our IT systems are inherently designed and regularly updated to try to ensure they remain as secure as possible. We use secure servers, firewalls, virus and ransom scanning software, and employ a team of IT professionals to support these systems. We have a framework in place for undertaking data protection impact assessments whenever a proposed new project or initiative involving our use of personal information is likely to result in a high risk to the individuals whose personal information is affected and in order to identify, manage and address any privacy risks posed.



Who do we disclose your personal information to and why?

We maintain comprehensive and detailed registers of all the 3rd parties with whom we share personal information that we are responsible for.

These registers include information on 3rd party service providers that we instruct and who process personal information on our behalf (such as payroll providers and business travel agencies – our data processors), and also 3rd parties we may otherwise share personal information with (such as benefits providers, tax or regulatory or government authorities – our data transfers).

The registers also include information regarding the countries/territories in which each those organisations are based.

Where we share personal information it is primarily with other organisations in countries/territories in which the Standard Bank Offshore Group companies are themselves based (Isle of Man, Jersey and Mauritius) and/or certain other countries/territories that are either part of the European Economic Area (EEA) or have been granted EU adequacy rulings from a data protection perspective (if different).

The only other countries/territories in which there are organisations to which we may routinely share certain limited staff personal information as required for the specific purposes for which it is required are:

- tax and/or regulatory and/or governmental and/or law enforcement/judicial authorities in your home country/territory or other countries/territories where we are legally obliged to do so;
- where you have used a recruitment agency/business and/or professional adviser/services business to engage and/or liaise with us on your behalf and that third party is in such a country/territory;
- the wider Standard Bank Group of companies (see [link tbc] for our different Standard Bank offices and their locations), including South Africa, where it is in our legitimate interests to do so to facilitate: Standard Bank Group communications to you; salary and benefit provision and delivery; strategic and organisational planning and management of our workforce generally; business intelligence management information generation; IT support services; the prevention and detection of crime; the safety of our clients, staff and the wider public; internal administrative purposes; training and monitoring purposes; and for handling enquiries, complaints and legal claims;
- limited sharing to the USA for service management solutions in supporting some of our information technology requirements;
- other business/professional services/product providers worldwide where this is in our legitimate interests to accommodate your working arrangements, provide you with benefits, and to support our business or in order for us to exercise, bring or defend a legal claim (see the Categories of other business, professional services and product providers table below);



- other banking and/or financial services and/or investment services providers and institutions worldwide where we are required to provide your personal information for cheque or payment or transaction processing; and
- other employer or educational organisations worldwide with whom you have indicated having past or present employment/education with and where we may seek to verify any past or present employment/education you have confirmed details of to us or to whom you ask us to provide references/ information on your behalf.

The foregoing provides a general summary of our register information in terms of where we presently share staff personal information and why, for more specific information please contact the Data Protection Officer.

Categories of other business, professional services and product providers This is a non-exhaustive list of the types of businesses with whom we share personal information:

Vendor category	Definition
Managed Services	A service/product supplier that manages and assumes responsibility for providing defined services/products to staff of the Standard Bank Offshore Group, for example, pension providers, business travel agents, and health and travel insurance providers.
Co-Managed	A partnership arrangement between a vendor and the Standard Bank Offshore Group companies in which they work together using each of their respective knowledge/specialist skills/systems to achieve the end goal, for example, local Telecoms companies.
Hardware/Software Supplier	Companies/individuals that specialise in providing the Standard Bank Offshore Group with appropriate software and hardware to support the business needs, such as Microsoft.
Professional Services	An organisation or professional that offers customised, knowledge based services to the Standard Bank Offshore Group companies. They include lawyers, recruitment agencies, accountants, and financial/benefits advisers.
Business Consultants	Used for various projects required to implement change initiatives for the Standard Bank Offshore Group companies, for example, changes to enhance staff experience or to implement new processes to ensure compliance with new legislation and regulation.



Safeguards when we share personal information

When we do share personal information with a data processor then we ensure we have a lawful basis for doing so, have a formal vetting procedure that we follow

to assess that data processor's ability to look after any personal information shared with them, ensure we have a written contract in place with them to apply appropriate safeguards to protect personal information to a standard and in a manner that provides us with sufficient guarantees as to the security of that personal information (we typically use standardised European Union model clauses processing agreements for that purpose to govern the data privacy elements of the relationship), and undertake ongoing monitoring of that relationship.

When we share personal information with another third party but not to process that personal information on our behalf then we ensure we have a lawful basis for doing so, have a formal procedure that we follow to consider and approve



the transfer beforehand, and we follow best practice guidelines in terms of our use of standardised European Union model clauses transfer agreements to govern the data privacy elements of the relationship whenever that is possible.

Where the personal information is to be shared with organisations outside of the EEA or those countries with adequacy rulings then we naturally consider such sharing of personal information as likely to result in a high risk to the privacy of the individuals whose data is being shared and we follow our procedures as outlined above, which include an assessment in these circumstances to ensure we can lawfully share and that adequate measures are taken to protect the personal information being shared.



Legal disclaimer

We reserve the right to disclose your personal information to governmental bodies, exchanges and other regulatory or self-regulatory organisations should we be required to do so by law or should we believe that such action is necessary to:

- comply with the law or with any legal process;
- exercise, protect and defend our legal rights and property;
- prevent fraud, theft or abuse; and/or
- protect your personal safety or property and that of our customers or the general public (if you provide false or deceptive information about yourself or misrepresent yourself as being someone else, we will disclose such information to the appropriate regulatory bodies and commercial entities).

In addition, we may disclose information, if required to do so, to any regulatory authorities in connection with any investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us to legal liability.



How long we keep your personal information for

We only hold personal information in a format which permits your identification for as long as is necessary for the purposes for which it was obtained.

Where legal requirements oblige us to retain records for a particular period of time then those periods are the minimum period for which we will retain the relevant record.

Comprehensive, local law compliant, record retention and disposal policies for all of the different types of records we hold exist for each of the three jurisdictions (Jersey, Isle of Man and Mauritius) in which the data controllers of the Standard Bank Offshore Group operate.



Your rights

You have a number of rights in respect to your personal information:

1. You have a right of access to your personal information;
2. You have a right to take action to rectify inaccurate personal information;
3. You have a right to erase personal information;
4. You have a right to restrict the processing of your personal information;
5. You have a right to data portability;
6. You have a right to object to processing of personal information (including direct marketing);
7. You have a right not to be subject to a decision based solely on automated processing of your personal information, including profiling, which produces legal effects/significantly affects you;
8. You have a right to seek compensation for any material or non-material damage caused by a breach of our statutory obligations to look after your personal information;
9. You have a right to lodge a complaint with a data protection supervisory authority; and
10. You have a right to an effective judicial remedy against us.

General information on each of these rights, with any applicable conditions or pre- requisites to their exercise, and how to exercise them can be obtained by contacting either P&C or the Data Protection Officer.

Further specific information can be obtained from our data protection supervisory authorities, the contact details for which are available below:

Isle of Man Information Commissioner - <https://www.inforights.im/>

Jersey Information Commissioner - <https://jerseyoic.org/>

Mauritius Data Protection Office - <https://dataprotection.govmu.org/>

When your personal information is subjected to any automated decision- making, including profiling, we will provide the information about the logic, the significance and envisaged consequences of that decision making for you, to allow you to exercise your right to object.

At this present time, we do not apply automated decision-making or profiling to your personal information, however, should this change in the future, we will update this Privacy Statement.



Right to change this privacy statement

We may change this privacy statement. We will publish all changes on our staff intranet. The latest version of our privacy statement will replace all earlier versions, unless otherwise stated.

Queries and complaints

If you have any queries or complaints about privacy, please contact your Standard Bank Offshore Group Data Protection Officer at the details provided on page 3.

Standard Bank Offshore Group companies contact details

Standard Bank Isle of Man Limited

Standard Bank House One Circular Road Douglas
Isle of Man IM1 1SB
Telephone: +44 (0)1624 643643
Email: personalbanking@standardbank.com

Standard Bank Jersey Limited

Standard Bank House 47–49 La Motte Street St Helier
Jersey JE2 4SZ
Telephone: +44(0)1534 881188 Email: sbj@standardbank.com

Standard Bank International Investments Limited

Standard Bank House 47–49 La Motte Street St Helier
Jersey JE2 4SZ
Telephone: +44(0)1534 881188 Email: sbsam@standardbank.com

Standard Bank Offshore Trust Company (Jersey) Limited

47–49 La Motte Street St Helier
Jersey JE2 4SZ
Telephone: +44(0)1534 881188 Email: trust@standardbank.com

Standard Bank Trust Company Mauritius Limited

Level 10, Tower A 1 CyberCity Ebene, Mauritius
Telephone: +230 402 6000
Email: sbtm@standardbank.com

Standard Bank Jersey Limited and Standard Bank Offshore Trust Company Jersey Limited are regulated by the Jersey Financial Services Commission. The entities are registered in Jersey as Company numbers 12999 and 9153 respectively. Melville Douglas is a registered business name of Standard Bank Jersey Limited. The business address for all entities is Standard Bank House, 47–49 La Motte Street, St Helier, Jersey, JE2 4SZ.

The above entities are wholly owned subsidiaries of Standard Bank Offshore Group Limited whose registered office is Standard Bank House, 47–49 La Motte Street, St Helier, Jersey, JE2 4SZ. Standard Bank Offshore Group Limited is a wholly owned subsidiary of Standard Bank Group Limited which has its registered office at 9th Floor, Standard Bank Centre, 5 Simmonds Street, Johannesburg 2001, Republic of South Africa.

Standard Bank Isle of Man Limited is licensed by the Isle of Man Financial Services Authority. Standard Bank House, One Circular Road, Douglas, Isle of Man, IM1 1SB. Registered in the Isle of Man No. 4713C.

Standard Bank Trust Company (Mauritius) Limited is regulated by the Financial Services Commission, Mauritius, to provide corporate and trust services and does not fall under the regulatory and supervisory purview of the Bank of Mauritius. Business registration number: C06021609. Level 10, Tower A, 1 Cyber City, Ebene, Mauritius.

The above entities are wholly owned subsidiaries of Standard Bank Offshore Group Limited whose registered office is Standard Bank House, 47–49 La Motte Street, St. Helier, Jersey, JE2 4SZ.