Our Privacy Notice for Commercial Banking and Global Banking and Markets Customers in the Kingdom of Bahrain

Effective from 12 February 2020

HSBC

PUBLIC

Before we begin

This notice (Privacy Notice) applies to information held about you and Connected Persons by HSBC Bank Middle East Limited Bahrain Branch and other members of the HSBC Group as data controllers, as described below. It explains what information we collect about you and Connected Persons, how we'll use that information, who we'll share it with, the circumstances when we'll share it, and what steps we'll take to make sure it stays private and secure. It continues to apply even if your agreement for banking or other products and services with us ends. It should also be read alongside your banking terms and conditions (or other applicable product or service terms and conditions), as these include sections relating to the use and disclosure of information.

Some of the links on our websites lead to other HSBC or non-HSBC websites with their own privacy notices, which may be different to this notice. You'll need to make sure you're happy with their privacy notices when using those other sites.

Wherever we've said 'you' or 'your', this means you, any authorised person on your account, anyone who does your banking or deals with us for you (e.g. trustees or executors, attorneys under a Power of Attorney) and other related people (including authorised signatories, partners, members and trustees).

Parts of this notice relate only to individuals, and we have highlighted this where relevant. This includes individuals whose business does not have a separate legal identity (e.g. sole traders and partners in a general partnership, but excluding limited companies and other forms of corporate entity).

Wherever we use the term "Connected Person(s)", this means individual(s) connected to you and could be any guarantor, a director, officer or employee of a company, partners or members of a partnership, any substantial owner, controlling person, or beneficial owner, trustee, settlor or protector of a trust, account holder or authorised signatory of a designated account, recipient of a designated payment, your attorney or representative, agent or nominee, individuals who are your clients, or any other persons with whom you have a relationship relevant to your relationship to the HSBC Group.

You must direct any individuals whose personal data we may collect and process, including Connected Persons, to this Privacy Notice and make sure they are aware, prior to providing their information to us or our obtaining their information, that we are using their information as described.

When we say 'we', we mean HSBC Group companies which act as a data controller in respect of your personal data. Unless otherwise stated below, the data controller for the purposes of this notice will be HSBC Bank Middle East Limited (P.O.Box 57, Manama, Bahrain).

What information we collect relating to you and Connected Persons

We'll only collect your information and information relating to Connected Persons, in line with relevant regulations and law. We may collect it from a range of sources and it may relate to any of our products or services you apply for, currently hold or have held in the past. We may also collect information about you and Connected Persons when you or they interact with us, e.g. visit our websites or mobile channels, call us or visit one of our branches, or ask about any of our products and services.

Some of this information will come directly from you and Connected Persons, e.g. when providing ID to open an account. It can also come from your financial advisor, lawyers, broker or other intermediary and other HSBC companies. We might also get some of it from publicly available sources.

The information we collect may include:

Information relating to you and Connected Persons that you provide to us, or which others provided to us on your behalf e.g.:

- where you're an individual, personal details (e.g. name, previous names, gender, date and place of birth). We'll also collect this information about Connected Persons;
- contact details (e.g. address, email address, position in company, landline and mobile numbers);

PUBLIC

- information concerning your identity including where you're an individual and, in the case of Connected Persons, photo ID, passport information, National ID card and nationality;
- market research (e.g. information and opinions expressed when participating in market research);
- user login and subscription data (e.g. login credentials for phone and online banking and mobile banking apps); and
- other information about you and Connected Persons that you've provided to us by filling in forms or by communicating with us, whether face-to-face, by phone, email, online, or otherwise.

Information we collect or generate about you and Connected Persons, e.g.:

- your financial information and information about your relationship with us, including the products and services you hold, the channels you and Connected Persons use and your and their ways of interacting with us, your ability to get and manage your credit, your payment history, transactions records, bank feeds, market trades, sort code and account numbers of customers' accounts, payments into your account including information concerning complaints and disputes and full beneficiary name, address and details of the underlying transaction;
- information we use to identify and authenticate you and Connected Persons, (e.g. signature and biometric information, such as voice for voice ID and additional information that we receive from external sources that we need for compliance purposes);
- geographic information (e.g. about which branches or ATMs you and Connected Persons use);
- information included in customer documentation (e.g. a record of advice that we may have given you);
- marketing and sales information (e.g. details of the services you receive and your preferences);
- cookies and similar technologies we use to recognise you and Connected Persons,
- remember preferences and tailor the content we provide;
- risk rating information (e.g. credit risk rating, transactional behaviour and underwriting information);
- investigations data (e.g. due diligence checks, sanctions and anti-money laundering checks, external intelligence reports, content and metadata related to relevant exchanges of information between and among you and individuals, organisations, including emails, voicemail, live chat);
- records of correspondence and other communications between you and your representatives and us, including email, live chat, instant messages and social media communications;
- information that we need to support our regulatory obligations (e.g. information about transaction details, detection of any suspicious and unusual activity and information about parties connected to you or these activities.

Information we collect from other sources relating to you and Connected Persons, e.g.:

- information you've asked us to collect for you (e.g. information about your accounts or holdings with other companies including transaction information); and
- information from third party providers (e.g. information that helps us to combat fraud or that relates to social interactions (including communications via social media, between individuals, organisations, prospects and other stakeholders acquired from companies that collect combined information).

How we'll use your information and information relating to Connected Persons

We'll only use information on you and Connected Persons where we have consent or we have another lawful reason for using it. These reasons include where we:

- need to pursue our legitimate interests such as to ensure compliance with our internal operational requirements or those of the HSBC Group (including credit and risk management, system or data base development, enhancement and planning, insurance, audit and administrative purposes);

PUBLIC

- need to process the information to carry out an agreement we have with you;
- need to process the information to comply with a legal obligation;
- believe the use of information as described is in the public interest (e.g. for the purpose of preventing or detecting crime); and
- need to establish, exercise or defend our legal rights.

The reasons we use your information and information relating to Connected Persons include:

- delivering our products and services;
- carrying out your instructions (e.g. to fulfil a payment request or make a change to your insurance policy);
- carry out checks in relation to your creditworthiness, managing our relationship with you, including (unless you tell us otherwise) telling you about products and services we think may be relevant for you;
- understanding how you use your accounts and services;
- providing banking operations support;
- preventing or detecting crime including fraud and financial crime (e.g. financing for terrorism and human trafficking);
- investigating and resolving complaints;
- providing security and business continuity;
- undertaking risk management;
- providing online banking, mobile apps and other online product platforms;
- undertaking product and service improvement;
- undertaking data analytics to better understand your circumstances and preferences so we can make sure we can provide you with the best advice and offer you a tailored service;
- protecting our legal rights and complying with our legal obligations;
- corresponding with lawyers, surveyors, valuers, other lenders, conveyancers and third party intermediaries;
- undertaking system or product development and planning, insurance, audit and administrative purposes; and
- recovering money which you owe.

Further details of how we'll use your information can be found in the Appendix on page 9.

How we make decisions about you

We may use automated systems to help us make decisions, (e.g. when you apply for products and services, to make credit decisions and to carry out fraud and money laundering checks). We may use technology that helps us identify the level of risk involved in customer or account activity (e.g. for credit, fraud or financial crime reasons, or to identify if someone else is using your card without your permission).

Individuals may have a right to certain information about automated decisions we make about them and may also have a right to request human intervention and to challenge the decision. More details can be found in the 'Rights of individuals' section below.

Tracking or recording what you say or do

To help keep you and your money safe, we may record details of your interactions (and the interactions of Connected Persons) with us. We may record and keep track of conversations with us including phone calls, face-to-face meetings, letters, emails, live chats, video chats and any other kinds of communication.

We may use these recordings to check your instructions to us, assess, analyse and improve our service, train our people, manage risk or to prevent and detect fraud and other crimes. We may also capture additional information about these interactions (e.g. telephone numbers that we are called from and information about

PUBLIC

devices or software that are used). We use closed circuit television (CCTV) in and around our sites and these may collect photos videos or voice recordings of you and Connected Persons.

Compliance with laws and regulatory compliance obligations

We'll use your information and information relating to Connected Persons to meet our compliance obligations, to comply with laws and regulations that HSBC Group companies are subject to and to share with our regulators and other regulators and authorities. This may include using information to help detect or prevent crime (including terrorism financing, money laundering and other financial crimes). We'll only do this on the basis that it's needed to comply with a legal obligation or it's in our legitimate interests and that of others.

Marketing and market research

We may use your information and information relating to Connected Persons to provide information about HSBC products and services, and also products and services from our partners and other relevant third parties. We may send marketing messages by post, email, telephone, text or secure messages. If you or a Connected Person wish to change how marketing messages are sent or wish to stop receiving these, please contact us in the usual way.

It may take us a short period of time to update our systems and records to reflect requests to stop receiving marketing messages, during which time you and Connected Persons may continue to receive marketing messages. Even if you tell us not to send marketing messages, we'll continue to use contact details to provide important information, such as changes to your terms and conditions or if we need to tell you, or a Connected Person, something to comply with our regulatory obligations.

We may use your information and information relating to Connected Persons for market research and to identify trends. Market research agencies acting on our behalf may get in touch with you or Connected Persons by post, telephone, email or other methods of communication to invite you or them to take part in research. We won't invite you or Connected Persons to take part in research using a communication method if you (or they) have asked us not to get in touch that way. Any responses that are provided whilst participating in market research will be reported back to us anonymously unless you or a Connected Person give us permission for the relevant details to be shared.

Who we might share information with

We may share your information and information relating to Connected Persons with others where lawful to do so including where we or they:

- need to in order to provide you with products or services you've requested (e.g. fulfilling a payment request);
- have a public or legal duty to do so (e.g. to assist with detecting and preventing fraud, tax evasion and financial crime);
- need to in connection with regulatory reporting, litigation or asserting or defending legal rights and interests;
- have a legitimate business reason for doing so (e.g. to manage risk, verify identity, enable another company to provide you with services you've requested, or assess your suitability for products and services);
- have asked you or a Connected Person for your permission to share it, and you (or they) have agreed.

We may share your information and information relating to Connected Persons for these purposes with others, including:

- other HSBC Group companies and any sub-contractors, agents or service providers who work for us or provide services to us or other HSBC Group companies (including their employees, sub-contractors, service providers, directors and officers);

PUBLIC

- any trustees, beneficiaries, administrators or executors;
- people who give guarantees or other security for any amounts you owe us;
- people you make payments to and receive payments from;
- your beneficiaries, intermediaries, correspondent and agent banks, clearing houses, clearing or settlement systems, market counterparties and any companies you hold securities in through us (e.g. stocks, bonds or options);
- other financial institutions, lenders and holders of security over any property or assets you charge to us, tax authorities, trade associations, credit reference agencies, payment service providers and debt recovery agents;
- any fund managers who provide asset management services to you and any brokers who introduce you to us or deal with us for you;
- any entity that has an interest in the products or services that we provide to you, including if they take on the risk related to them;
- any people or companies where required in connection with potential or actual corporate restructuring, merger, acquisition or takeover, including any transfer or potential transfer of any of our rights or duties under our agreement with you;
- law enforcement, government, courts, dispute resolution bodies, our regulators, auditors and any party appointed or requested by our regulators to carry out investigations or audits of our activities;
- other parties involved in any disputes, including disputed transactions;
- fraud prevention agencies who'll also use it to detect and prevent fraud and other financial crime and to verify your identity;
- anyone who provides instructions or operates any of your accounts, products or services on your behalf (e.g. Power of Attorney, lawyers, intermediaries, etc);
- anybody else that we've been instructed to share your information with by you, or anybody else who provides instructions or operates any of your accounts on your behalf; and
- our card processing supplier(s) to carry out credit, fraud and risk checks, process your payments, issue and manage your card.

Sharing aggregated or anonymised information

We may share aggregated or anonymised information within and outside of the HSBC Group with partners such as research groups, universities or advertisers. Neither you nor Connected Persons will be able to be identified from this information (e.g. we may share information about general spending trends in the Kingdom of Bahrain to assist in research).

How long we'll keep information

We will keep this information for as long as you keep banking with us and using our platforms (e.g. our website and mobile apps). We may keep this information after you stop banking with us or stop using our platforms, for instance, to respond to enquiries and complaints, as required by law and regulations or to protect our interests.

This enables us to comply with legal and regulatory requirements or to use your information where we need to for our legitimate purposes such as managing your account and dealing with any disputes or concerns that may arise.

We may need to retain information for a longer period where we need the information to comply with regulatory or legal requirements or where we may need it for our legitimate purposes (e.g. to help us respond to queries or complaints, fighting fraud and financial crime, responding to requests from regulators, etc.).

If we don't need to retain information for this period of time, we may destroy, delete or anonymise it more promptly.

PUBLIC

Where you receive products and services from third parties to whom HSBC has introduced you, those third parties may keep your information, and information relating to Connected Persons, in line with additional terms and conditions that apply to their product and services.

Transferring information overseas

Your information and information relating to Connected Persons may be transferred to and stored in locations outside the Kingdom of Bahrain, including countries that may not have the same level of protection for personal information. When we do this, we'll ensure it has an appropriate level of protection and that the transfer is lawful. We may need to transfer information in this way to carry out our contract with you, to fulfil a legal obligation, to protect the public interest and/or for your or our legitimate interests. In some countries the law might compel us to share certain information (e.g. with tax authorities). Even in these cases, we'll only share information with people who have the right to see it.

You can obtain more details of the protection given to your information (and information relating to Connected Persons) when it's transferred outside the Kingdom of Bahrain by contacting us using the details in the 'More details about your information and information about Connected Persons' section on page 8.

Rights of individuals

Individuals have a number of rights in relation to the information that we hold about them. These rights include:

- the right to access information we hold about them and to obtain information about how we process it;
- in some circumstances, the right to withdraw their consent to our processing of their information, which they can do at any time. We may continue to process their information if we have another legitimate reason for doing so;
- in some circumstances, the right to receive certain information they have provided to us in an electronic format and/or request that we transmit it to a third party;
- the right to request that we rectify their information if it's inaccurate or incomplete;
- in some circumstances, the right to request that we erase their information. We may continue to retain their information if we're entitled or required to retain it; and
- the right to object to, and to request that we restrict, our processing of their information in some circumstances. Again, there may be situations where individuals object to, or ask us to restrict, our processing of their information but we're entitled to continue processing their information and/or to refuse that request.

Individuals (including Connected Persons) can exercise their rights by contacting us using the details set out in the 'More details about your information and information relating to Connected Persons' section on page 8.

Credit reference checks, fraud and money laundering

Credit reference checks

If you apply for new products or services (including credit like a loan or credit card), we may perform credit and identity checks on you (and certain Connected Persons) from the Bahrain Credit Reference Bureau operating under the trade name The Benefit Company BSC (Closed) ("**the CRA**"). When you use our banking services, we may also make periodic searches at the CRA to manage your account with us.

To do this, we'll supply your information (and information of certain Connected Persons) to the CRA and they'll give us information about you and them. This will include information from your credit application and about your financial situation and financial history (and the financial situation and history of relevant Connected Persons). The CRA will supply us with both public (including the electoral register) and shared credit information, financial situation, history and fraud prevention information.

PUBLIC

We may use this information to:

- assess if we can offer you credit and whether you can afford to take the product you applied for;
- verify the accuracy of the data you've provided to us;
- prevent criminal activity, fraud and money laundering; manage your account(s); trace and recover debts; and
- ensure any offers provided to you are appropriate to your circumstances.

We'll continue to exchange information about you (and Connected Persons) with the CRA while you have a relationship with us. We'll also inform the CRA about your repayment history. If you borrow and do not repay in full and on time, the CRA will record the outstanding debt. This information may be supplied to other organisations by the CRA.

When the CRA receives a search request from us they'll place a search footprint on your credit file (or that of the relevant Connected Persons) that may be seen by other lenders. If you apply for a bank account or credit (such as where you apply for a loan or credit card), we'll get details of your credit history from the CRA (and share information about you and the Connected Persons with the CRA) and use this information to work out how much you can afford to borrow or pay back. We may also carry out further credit checks on you and the Connected Persons while you're a customer to maintain an accurate and up-to-date record of your credit history. We may use this information to verify the accuracy of the information you've provided to us, to prevent criminal activity, fraud and money laundering, to manage your account(s), trace and recover debts and to ensure any offers provided to you are appropriate to your circumstances.

If you tell us that you have a financial associate (or, where you are an individual, a spouse), we'll link your records together. You should discuss this with them, and share this information with them before submitting the application. The CRA will also link your records (and those of Connected Persons) together and these links will remain on your and their files until you or the relevant individual successfully files for a disassociation with the CRA to break that link.

To comply with the law and for our own legitimate interest to enable us to assess and manage risk, we can share details about your financial situation and financial history, and the financial situation and history of Connected Persons with the CRA, fraud prevention agencies, etc. This includes information on any bank accounts or credit you have with us, including:

- how you manage your bank accounts or credit;
- if you owe us money;
- if we have concerns about financial crime; and
- if you haven't kept up with your payments or paid off what you owe us (unless there's a genuine dispute over how much you owe us), or if you've agreed and stuck to a repayment plan.

Fraud prevention agencies

We'll carry out checks with fraud prevention agencies for the purposes of preventing fraud and money laundering, and to verify your identity and the identity of Connected Persons before we provide products and services to you. These checks require us and these agencies to process information about you and Connected Persons.

The information you provide or which we've collected from you, or on your behalf, including from Connected Persons or received from third parties, will be used to carry out these checks in order to prevent fraud and money laundering, and to verify your identity and the identity of Connected Persons. This includes information such as name, address, date of birth, contact details, financial information, employment details, and device identifiers (e.g. IP address).

We and fraud prevention agencies may also enable law enforcement agencies to access and use information about you and Connected Persons to detect, investigate and prevent crime.

PUBLIC

We process this information on the basis that we have a legitimate interest in preventing fraud and money laundering and to verify your identity and the identity of Connected Persons. This enables us to protect our business and to comply with laws that apply to us. This processing is also a contractual requirement of any of our products or services you use.

Consequences of processing

If we, or a fraud prevention agency, have reason to believe there's a fraud or money laundering risk, we may refuse to provide the services and credit you've requested. We may also stop providing existing products and services to you and/or Connected Persons. A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services to you and Connected Persons. The information we hold about you and information relating to Connected Persons, could make it easier or harder for you or them to get credit in the future.

What we need from you

You're responsible for making sure the information you give us, information which is provided by Connected Persons, or information which is otherwise provided on your behalf is accurate and up to date, and you must tell us if anything changes as soon as possible, and in any event, within 30 days in writing.

Where:

- you fail to provide information that HSBC reasonably requests; or
- you withhold or withdraw any consents which HSBC may need to provide you with banking or other products and services; or
- HSBC or a member of the HSBC Group has suspicions regarding the possible commission of financial crime or you present a potential financial crime risk to a member of the HSBC Group,

HSBC may:

- be unable to provide new, or continue to provide all or part of the, services to you and reserves the right to terminate its business relationship with you;
- take actions necessary for HSBC or a member of the HSBC Group to meet its compliance obligations; and/or
- block, transfer or close your account(s).

In addition, the failure to supply your or your Connected Person's tax Information may result in HSBC making its own decision with respect to your status, including whether to report you to a tax authority, and may require HSBC or other persons to withhold and pay such amounts as may be legally required by any tax authority.

You should direct Connected Persons to this Privacy Notice and make sure they understand how we use their information as described in it prior to providing their information to us, or our obtaining their information from other sources. You should also draw their attention to the section on their rights.

How we keep information secure

We use a range of measures to keep information safe and secure which may include encryption and other forms of security. We require our staff and any third parties who carry out any work on our behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate measures for the use and transfer of information.

More details about your information and information relating to Connected Persons

To obtain further information on anything we've said in this Privacy Notice please email HSBC Bank Middle East Limited at cust.exp.corp.bh@hsbc.com,

This Privacy Notice may be updated from time to time and the most recent version can be found at www.hsbc.com.bh

PUBLIC

Appendix – How we process information about you and Connected Persons

We'll use your information and information about Connected Persons for purposes, including:

to deliver our products and services: to administer your accounts, process your transactions. We'll do this in order to perform our contract with you;

to provide banking operations support: to enable the provision and function of our banking services in line with regulation, laws and customer rights and interests (e.g. complaints management and exit management). We do this to comply with our legal obligations, to perform our contract with you and because it's in our legitimate interest;

to prevent and detect crime including (e.g. fraud, terrorist financing and money laundering): this will include monitoring, mitigation and risk management, carrying out customer due diligence, name screening, transaction screening and customer risk identification. We do this to comply with our legal obligations and because it's in our legitimate interest. We may share your information and information relating to Connected Persons with relevant agencies, law enforcement and other third parties where the law allows us to for the purpose of preventing or detecting crime. Additionally, we and other financial institutions may take steps to help prevent financial crime and manage risk. We'll do this because we have a legitimate interest, a legal obligation to prevent or detect crime or it's in the public interest. We may be required to use your information and information relating to Connected Persons to do this, even if you or they have asked us to stop using your/their information. That could include (among other things):

- screening, intercepting and investigating any payments, instructions or communications you send or receive (including drawdown requests and application forms);
- investigating who you're paying or who's paying you (e.g. checks on payments into and out of your account and other parties related to those payments);
- passing information to relevant agencies if we think you, Connected Persons and others acting on your behalf have given us false or inaccurate information, or we suspect criminal activity;
- combining the information, we have about you and information relating to Connected Persons with information from other HSBC companies to help us better understand any potential risk;
- checking whether the people or organisations you're paying or receiving payments from are who they say they are, and aren't subject to any sanctions.

to undertake risk management: to measure, detect and prevent the likelihood of financial, reputational, legal, compliance or customer risk. This includes credit risk, traded risk and operational risk. We'll do this because we have a legitimate interest in ensuring that we carry out a proper risk assessment prior to providing credit or other finance;

to provide Online Banking, mobile apps and other online product platforms: to allow us to provide you (and those you authorise) with access to HSBC online platforms and mobile apps. The platform may allow you and your authorised users to directly or indirectly communicate with us, apply for products and services online and verify customer ID and proof of address. The lawful basis for using your information and information relating to Connected Persons for this purpose is to perform our contract with you or that processing for this purpose is in our legitimate interest;

to provide product and service improvement: to identify possible service and product improvements by analysing your information and information relating to Connected Persons. Where we provide you with aggregated information services, we'll use your information and information relating to Connected Persons to understand how you use these products which may include your transactional information from other financial institutions to help improve our products and services. The lawful basis for processing your information and information relating to Connected Persons for this purpose is our legitimate interest. We do this to improve our products and services to best meet the need of our customers;

to undertake data analytics and to provide tailored services: to identify relevant opportunities to promote products and services to existing or prospective customers by analysing your information and information

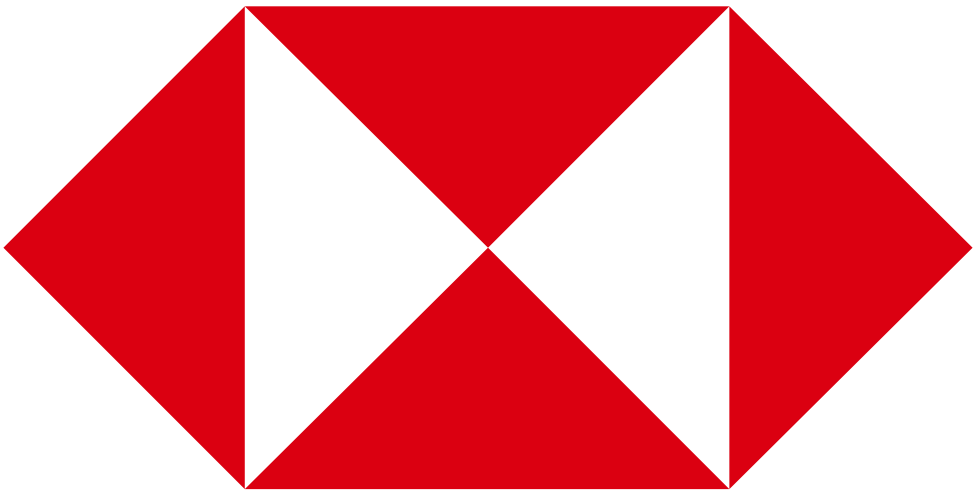
PUBLIC

relating to Connected Persons. This may include reviewing historical customer transactional behaviour, comparison of customer activity or (if you use Connected Money) it may include an analysis of your transactional information from other financial institutions. We do this to help us provide you with products and services we think will be of most relevance to you. The lawful basis for using your information and information relating to Connected Persons in this way is our legitimate interest;

to undertake marketing: to provide you with information about HSBC products and services, and also products and services from our partners and other relevant third parties. The lawful basis for this is our legitimate interest. We may need your consent (or the consent of Connected Persons) to communicate by certain channels and we'll always make sure we get this where we need to. You and Connected Persons can change your mind on how you receive marketing messages or choose to stop receiving them at any time. To make that change, contact us in the usual way;

to protect our legal rights: to protect our legal rights, e.g. in the case of defending or the protection of legal rights and interests (e.g. collecting money owed, enforcing or protecting our security or defending rights of intellectual property); court action; managing complaints or disputes; in the event of a restructuring of companies or other mergers or acquisitions. This may be in connection with action taken against you or other persons (e.g. joint borrowers or persons who give a guarantee or other security for your obligations to us. We'd do this on the basis that it's in our legitimate interest).

PUBLIC



PUBLIC