

Our privacy notice



Before we begin

This Privacy Notice applies to personal information held by M&S Bank and M&S Bank companies outlined below. M&S Bank is a trading name of Marks & Spencer Financial Services plc, which is part of the HSBC Group.

This notice explains what information we collect about you and how we'll use it. It will also explain who we'll share your information with and when, plus what we'll do to make sure it stays safe and secure. It continues to apply even if your agreement for banking, insurance or other products and services with us ends. It should also be read alongside your product terms and conditions.

This Privacy Notice covers any personal products or services you have with us. This includes savings, travel money, loans, credit cards, Sparks pay, investments and insurance. If you also bank with other parts of the HSBC Group (for example, HSBC business banking, first direct, or HSBC in any other countries), they'll provide you with information separately where required.

Some links on our websites lead to other HSBC Group or non-HSBC websites, including the Marks and Spencer Group, with their own privacy notices, which may be different to this one. You'll need to make sure you're happy with their privacy notices when using those 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 (for example, trustees, executors or attorneys under a Power of Attorney) and other related people (including authorised signatories, partners, members and trustees). If you're an insurance customer it also means you, named insured parties or beneficiaries under your policy, dependants, claimants and other third parties involved in an insurance policy or claim (such as witnesses).

When we say 'we,' we mean:

M&S Bank, who is the data controller for savings accounts, travel money, credit cards, Chargecard, Budgetcard, Privilege Card, Foreign Exchange, Personal Reserve, Sparks pay, Club Rewards, loans, World Selection and all insurance products;

Marks and Spencer Unit Trust Management Limited, who is the data controller for M&S High Income Fund, M&S Worldwide Managed Fund, M&S UK Selection Portfolio and M&S UK 100 Companies Fund; and

Marks & Spencer Financial Services plc, who is the data controller for the M&S Corporate ISA.

The data controller is responsible for deciding how your information is used and ensuring it is private and secure.

The address for the companies set out in this notice is Kings Meadow, Chester CH99 9FB. If you'd like to get in touch with us, you can also find additional contact details in the 'More details about your information' section below.

What information we collect

We'll only collect information about you as allowed by regulation and law. We may collect it from a range of places 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 when you interact with us. This includes when you visit our websites or mobile channels, call us or ask about any of our products and services.

Some of it will come directly from you, for example, when you provide ID to open an account. It can also come from your financial advisor, other HSBC companies, the insurance company which provides the insurance policies we offer, the Marks and Spencer Group or other places you've asked us to get information from. We might also get some from publicly available places. The information we collect will depend on the type of product you hold. It may include:

Information that you provide to us, such as:

- personal details, for example, names, gender, date and place of birth;
- contact details, for example, address, email address, and telephone numbers;
- information about your identity, for example, photo ID, passport information, National Insurance number, National ID card and nationality;
- market research, for example, information and opinions given;
- user login and subscription data, for example, login details for phone, Internet Banking and Mobile Banking apps;
- other information about you that you give us when you fill forms in or by communicating with us, whether face-to-face, by phone, email, online, or otherwise.

Information we collect or provide about you, such as:

- your financial information and information about your relationship with us. This includes the products and services you hold, the channels you use, how you deal with us, your ability to get and manage credit, your payment history, transactions records, market trades, and information about complaints and disputes;
- information we use to identify you, for example, your signature and other information, such as your voice for voice ID, or additional information that we receive from external sources that we need for compliance purposes;
- information about where you live and where you use our products and services, for example, which cash machines you use;

- information included in customer documentation, for example, a record of advice that we may have given you;
- marketing and sales information, for example, details of the services you receive and your preferences;
- information about your device or the software you use, for example, its IP address, technical specification and uniquely identifying data;
- cookies and similar technologies we use to recognise you, remember your preferences and tailor the content we provide to you – our cookie policy contains more details about how we use cookies and can be found at marksandspencer.com/bankcookiepolicy
- risk rating information, for example, credit risk rating, transactional behaviour and underwriting information;
- investigations data, for example, due diligence checks, sanctions and anti-money laundering checks, external intelligence reports, content and metadata related to relevant exchanges of information between and among individuals and/or organisations, including emails, voicemail, live chat;
- records of correspondence and other communications between us;
- information we need to support our regulatory obligations, for example, detection of any suspicious and unusual activity and information about parties connected to you or these activities.

Information we collect from other places, such as:

- information you've asked us to collect for you, for example, details about your accounts with us or other companies including transaction data;
- information from third-party providers that helps us to stop fraud or that relates to your social interactions. This includes your communications via social media, between individuals, organisations, prospects and other stakeholders acquired from companies that collect combined information;
- information from the Marks and Spencer Group, for example, information about the transactions you undertake using your Sparks card (irrespective of how you pay), information relating to your membership of the M&S Loyalty Scheme;
- if our relationship arises out of an insurance policy or claim, we may also collect information about:
 - your insurance application where you applied via a comparison website or aggregator
 - your medical records, with your agreement;
 - your insurance claims history;
 - other parties involved in your insurance policy or claim;
 - publicly available sources.

How we'll use your information

We'll only use your information if we have your consent or we have another lawful reason for using it. These reasons include:

- if we need to pursue our legitimate interests;
- to enter into or carry out an agreement we have with you;
- where we are required to by law;
- where we believe it's in the public interest for us to do so, for example, to help prevent or detect crime;
- to establish, utilise or defend our legal rights;
- for insurance purposes.

The reasons we use your information include to:

- provide you with our products and services;
- carry out your wishes, for example, make a payment request or a change to your insurance policy;
- carry out credit checks;
- understand how you use your accounts and services;
- help us with our banking processes;
- prevent or detect crime including fraud and financial crime, for example, financing for terrorism and human trafficking;
- ensure security and business continuity;
- manage risk;
- provide online services such as Internet Banking and mobile apps;
- market our products and services to you and others;
- improve our products and services, from seeing how you use them;
- help us 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;
- protect our legal rights and comply with our legal obligations;
- correspond with solicitors, surveyors, valuers, other lenders, conveyancers and third-party intermediaries;
- carry out system or product development and planning, insurance, audit and administrative purposes;
- if our relationship is because of an insurance policy or claim, we will also use your information to:
 - look at your insurance application and provide you with a quote;
 - handle or monitor any claims that you make or which arise under your insurance

policy;

- where relevant, bring a claim against a third party;
- apply for and claim on our own insurance policies. Further details of how we'll use your information can be found in the Appendix below.

How we make decisions about you

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

You may have a right to certain information about how we make these decisions. You may also have a right to request human intervention and to challenge the decision. More details can be found in the 'Your rights' section below.

Tracking or recording what you say or do

We want to help keep you and your money safe. To do this we may store details of your interactions with us. We may also 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 to check your instructions to us, analyse and improve our service, train our people, manage risk or to prevent and detect fraud and other crimes. We may also store additional information about these interactions, for example, telephone numbers that you call us from and information about the devices or software that you use. We use closed circuit television (CCTV) in and around our offices and these may collect photos or videos of you or record your voice.

Our websites, apps, and other digital products may also track and record your interactions with them. This is to help:

- keep you safe;
- us provide or improve services and features;
- keep our services secure;
- help make your visit more personal,
- support our marketing.

Some tracking is optional. For more details, please refer to our relevant website, app or other digital privacy notices and cookies notices.

Compliance with laws and regulatory compliance obligations

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

Marketing

We may use your information to provide you with details about our products and services, and also products and services from Marks and Spencer Group and other third parties. We may send you marketing messages by post, email, telephone, text, secure messages or through social media. You can change your mind on how you receive marketing messages or choose to stop receiving them at any time. To make that change, please contact us in the usual way.

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

Market research

We may use your information for market research and to identify trends. Market research agencies acting on our behalf may get in touch with you to invite you to take part in research. We won't invite you to take part in research using a communication method if you've asked us not to get in touch that way. Any responses you provide will be reported back to us anonymously unless you give us permission for your details to be shared. If you do not wish to be contacted for market research purposes, please let us know by using the details set out in the 'More details about your information' section below.

Who we might share your information with

We may share your information 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 asked for;
- need to in order to provide you with your insurance policy or to administer your claim;
- have a public or legal duty to do so, for example, to help with detecting and preventing fraud, tax evasion and financial crime;
- need to for any regulatory reporting, litigation or asserting or defending legal rights and interests;
- wish to send marketing to you or others, where you've given your permission, or it's within our or their legitimate interest to do so;
- have a legitimate business reason for doing so, for example, to manage risk, confirm your identity, enable another company to provide you with services you've asked for, or check your suitability for products and services;
- have asked you for your permission to share it, and you've agreed.

We may share your information 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);

- any joint account holders, trustees, beneficiaries 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, for example, stocks, bonds or options;
- other financial institutions, lenders and holders of security over any property 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;
- anybody who provides marketing services to us;
- any people or companies 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 asked for 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 confirm your identity;
- anyone who provides instructions or operates any of your accounts on your behalf, for example, Power of Attorney, solicitors, intermediaries, etc.;
- anybody else that we've been asked to share your information with by either you, a joint account holder or anybody else who provides instructions or operates any of your accounts on your behalf;
- our third party supplier(s) to carry out credit, fraud and risk checks, process payments, issue cards and documentation and to service your account;
- insurance providers who may use this information to apply discounts or offers that you may be entitled to from time to time as an M&S Bank customer, carry out analysis and research, fraud prevention and to help to assess insurance applications;
- if our relationship is because of an insurance policy or claim, we will also share your information with:
 - other parties involved in providing your insurance policy such as the intermediary or the insurer who provides your policy. For further details, please refer to your policy documentation. You can also refer to marksandspencer.com/bank for more information.
 - third parties involved in the administration of the relevant insurance policy or claim including loss adjusters, claims handlers, private investigators, experts and our advisers; and

- where relevant, medical experts and rehabilitation providers.

In addition to the above we will also share information about you with the Marks and Spencer Group and any agents, partners or service providers acting on their behalf. This will include details of your credit and/or store card transactions so:

- we can provide you with the benefits and services which you may be entitled to receive by holding M&S Bank products or services, for example, providing benefits associated with the loyalty scheme.
- they can use data analytics to profile your interests and decide if particular products or services may be of interest to you and send you offers (unless you ask them not to)
- you can be provided with the rewards you may be entitled to receive if you are a member of the M&S Loyalty Scheme which is subject to separate terms and conditions (bank.marksandspencer.com/pdf/LoyaltyTermsAndConditions.pdf)

For further information on how Marks and Spencer Group use your information please refer to their privacy notice available at marksandspencer.com.

Online advertising

When we advertise our products and services on the internet, we may share your information with our advertising partners. For example, when we use social media for marketing purposes, your information may be shared with the social media platforms so that they can check if you also hold an account with them. If you do, we may ask the advertising partner or social media network:

- to use your information to send our adverts to you, for example, because we think that you might be interested in a new service that we offer;
- to exclude you from receiving our adverts, for example, because the advert is for a service that you already use;
- to advertise to people who have a similar profile to you, for example, if we discover that one of our services is particularly useful to people with similar interests to the ones on your social media profile, we may ask our advertising partner or the social media network to send our adverts for that service to people who share your interests.

You can contact us if you don't wish us to share your personal data for online advertising. For more information, see 'Your rights' below.

Social media platforms also allow you to indicate your preferences to them about the advertising you receive on their platforms. Please contact your social media platforms for more information.

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. You won't be able to be identified from this information, for example, we may share information about general spending trends in the UK to help in research.

How long we'll keep your information

We keep your information in line with our data retention policy. For example, we'll normally keep your main banking information for a period of seven years from when our relationship with you ends. This allows us to comply with legal and regulatory requirements or use it 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 keep your 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, for example, to help us answer queries or complaints, fighting fraud and financial crime, answer requests from regulators, etc.

If we don't need to keep information for this length of time, we may destroy, delete or anonymise it sooner.

Transferring your information overseas

Your information may be transferred to and stored in locations outside the United Kingdom or the European Economic Area (EEA), 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 in line with applicable legal requirements. We may need to transfer your information in this way to carry out our contract with you, to fulfil a legal obligation, to protect the public interest and/or for our legitimate interests. In some countries, the law might compel us to share certain information, for example, with tax authorities. Even in these cases, we'll only share your information with people who have the right to see it.

You can get more details of the protection given to your information when it's transferred outside the United Kingdom or the EEA by contacting us using the details in the 'More details about your information' section below.

The EEA is made up of all member states of the European Union and Iceland, Liechtenstein and Norway.

Your rights

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

- the right to access information we hold about you and to get information about what we do with it;
- in some circumstances, the right to withdraw your consent to our processing of your information, which you can do at any time. We may continue to process your information if we have another legitimate reason for doing so;
- in some circumstances, the right to receive certain information you have provided to us in an electronic format and/or ask that we send it to a third party;
- the right to ask that we correct your information if it's inaccurate or incomplete;

- in some circumstances, the right to ask that we delete your information. We may continue to keep your information if we're entitled or required to keep it;
- the right to object to, and to request that we limit, our processing of your information in some circumstances. Again, there may be situations where you object to, or ask us to limit, our processing of your information but we're entitled to continue and/or to refuse that request.

You can exercise your rights by contacting us using the details set out in the 'More details about your information' section below. You also have the right to complain to the UK Information Commissioner's Office, by visiting ico.org.uk, or to the data protection regulator in the country where you live or work.

Credit reference checks, fraud and money laundering

Credit reference checks

If you apply for new products or use our services, we may carry out credit and identity checks on you with one or more credit reference agencies (CRAs). When you use our banking services, we may also make periodic searches at CRAs to manage your account with us.

To do this, we'll give your personal information to CRAs and they'll give us information about you. This will include information from your credit application and about your financial situation and financial history. CRAs will supply us with both public (including the electoral register) and shared credit information, financial situation, history and fraud prevention information.

We may use this information to:

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

We'll continue to exchange information about you with CRAs while you have a relationship with us, including details of your repayment history. If you borrow and don't make payment as per your agreement, CRAs will record the outstanding debt. This information may be supplied to other organisations by CRAs.

When CRAs receive a search request from us they'll place a search footprint on your credit file. This may be seen by other lenders. If you apply for an account or any other credit, we'll get details of your credit history from a CRA (and share information about you with them) 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 while you're a customer to maintain an accurate and up-to-date record of your credit history. We may use your information to confirm the accuracy of any details you've given 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.

If you're making a joint application, or tell us that you have a spouse or financial associate, we'll link your records together. You should discuss this with them, and share this information with them before submitting the application. CRAs will also link your records together and these links will remain on your and their files until you or your partner successfully files for a disassociation with the CRAs to break that link.

The identities of the CRAs, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail on their websites. They've created a joint document called the Credit Reference Agency Information Notice (CRAIN) which is accessible from each of the three CRAs – going to any of these three links will take you to the same CRAIN document:

Credit reference agencies:

- Transunion – transunion.co.uk/crain
- Equifax – equifax.co.uk/crain
- Experian – experian.co.uk/crain

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 with CRAs, fraud prevention agencies, etc. This includes information on any accounts or credit you have with us, including:

- how you manage your accounts or credit;
- if you owe us money;
- if we have concerns about financial crime;
- if you haven't kept up with your payments or paid off any amount 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 before we provide products and services to you. These checks require us to process personal information about you.

The personal information you provide or which we've collected from you, 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.

We'll process personal information, such as your name, address, date of birth, contact details, financial information, employment details, and device identifiers (for example, IP address).

We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

We process your personal data on the basis that we have a legitimate interest in

preventing fraud and money laundering and to verify your identity. 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.

Fraud prevention agencies can hold your personal data for different periods of time. If they're concerned about a possible fraud or money laundering risk, your data can be held by them for up to six years.

As part of the processing of your personal data, decisions may be made by automated means. This means we may automatically decide that you pose a fraud or money laundering risk if our processing reveals your behaviour to be consistent with money laundering or known fraudulent conduct, or is inconsistent with your previous submissions, or you appear to have deliberately hidden your true identity.

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 asked for. We may also stop providing existing products and services to you. A record of any fraud or money laundering risk will be kept by the fraud prevention agencies. This may be used to enhance fraud detection models and may also result in others refusing to provide services to you. The information we hold about you could make it easier or harder for you to get credit in the future.

To find out more about credit and fraud checks, read our 'Understanding credit scoring, credit and fraud prevention agencies' leaflet. You can get it from our website or you can request a paper copy by contacting us in your preferred way.

To find out more about our fraud prevention agencies and how they use your information, please visit each agency directly:

CIFAS - cifas.org.uk/fpn

Experian Ltd - experian.co.uk/privacy-and-your-data.html

Synectics Solutions Ltd - synectics-solutions.com/privacy

National Hunter - nhunter.co.uk/privacypolicy

BioCatch - biocatch.com/privacy-policy

LexisNexis (ThreatMetrix) - risk.lexisnexis.com/privacy-policy

Facebook

When you use any HSBC Page on Facebook, including the page for M&S Bank, Meta Platforms Ireland Limited (previously known as Facebook Ireland Limited) and HSBC collect information about you. This includes:

- what you click on: if you start a Messenger conversation;
- what you view: when you hover over a link or have an event page on screen;
- what you say: like comments or reactions;
- your actions: like sharing or recommending;

- your location: Country or region. This is not your precise location unless you have provided this in your user profile and you are logged-in;
- your device and internet connection;
- your Facebook profile details and user ID;

HSBC, including M&S Bank, has access to this information to use for reporting, insights and marketing purposes and so does Meta Platforms Ireland. This helps HSBC improve our offering on Facebook and create better marketing. HSBC may also see this information if HSBC has communicated with you on Facebook. HSBC does this because it helps us know who we're speaking to.

If you've allowed us to use cookies that support our marketing, HSBC and Meta Platforms Ireland can collect this information when you use HSBC's site too. To learn more, or to switch this off, visit our Cookies Notice at hsbc.co.uk/cookie-notice. You can control which cookies you allow by selecting "Manage Cookies".

Meta Platforms Ireland is a 'joint controller' with us in law for processing where we collect information about you:

- From your actions on our Facebook page.
- Through the Facebook pixel on our website.

We and Facebook have agreed to share some responsibilities to protect your personal data, by:

- Making sure we each have a legal basis for joint processing.
- Honouring your legal rights in respect of your data.
- Ensuring security of joint processing.

You can contact HSBC about how we do this. You can also contact Meta Platforms Ireland about what they do. This includes exercising your legal rights in respect of the data Facebook collects and retains itself.

Further details of how Meta Platforms Ireland processes your personal information, the legal basis it relies on, your rights and their contact details can be found at: facebook.com/about/privacy.

What we need from you

You're responsible for making sure the information you give us is accurate and up to date, and you must tell us if anything changes as soon as possible. If you provide information for another person on your account, product or service (for example, a joint account holder, a beneficiary under an insurance policy or a dependant), you'll need to direct them to this notice and make sure they agree to us using their information as described in it.

How we keep your information secure

We use a range of measures to keep your 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

If you'd like further information on anything in this Privacy Notice, contact us at M&S Bank, PO Box 10565, 51 Saffron Road, Wigston, LE18 9FT or M&S Bank, Kings Meadow, Chester CH99 9FB and marking the letter for the attention of Rights of Individuals Fulfillment. Alternatively, you can contact us via the M&S Banking App where you can chat to us 24/7 or via telephone banking.

This Privacy Notice may be updated from time to time and the most recent version can be found at marksandspencer.com/bankprivacynotice.

This notice was last updated in January 2023.

Appendix - How we process your information

We will use your information for purposes including:

- To deliver our products and services (including insurance): administer your accounts, or process your transactions. We'll do this in order to perform our contract with you;
- Banking operations support: we'll use your information to enable the provision and function of our banking services in line with regulation, laws and customer rights and interests, for example, complaints management and exit management. The lawful reasons for processing these are legitimate interest, legal obligation and in order to perform our contract with you;
- To prevent and detect crime including, for example, 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 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 to do this, even if you've asked us to stop using your 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, for example, 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've given us false or inaccurate information, or we suspect criminal activity;
 - combining the information we have about you 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.
- Risk management: we'll use your information to measure, detect and prevent the likelihood of financial, reputational, legal, compliance or customer risk. This includes credit risk, traded risk, operational risk and insurance risk (for example, for underwriting or claims management purposes). We'll do this because we have a legitimate interest in ensuring that we carry out a proper risk assessment prior to providing credit, insurance or other finance;
 - Internet Banking, mobile apps and other online product platforms: we'll use your information to allow us to provide you with access to M&S Bank online platforms and mobile apps (for example, the M&S Banking App). This includes information you provide to us, directly or indirectly communicate with us through mobile apps, such as using Internet Banking, or when applying for products and services online. The lawful basis for using your information for this purpose is to perform our contract with you or that processing for this purpose is in our legitimate interest;
 - Product and service improvement: we'll analyse your information to identify possible service and product improvements. Where we provide you with aggregated information services, we'll use your information 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 for this purpose is our legitimate interest. We do this to improve our products and services to best meet the need of our customers;
 - Data analytics: we'll analyse your information to identify relevant opportunities to promote products and services to existing or prospective customers and to understand how our products and services are used. For example, this may include reviewing historical customer transactional behaviour comparison of customer activity or 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 in this way is our legitimate interest;
 - Marketing: we'll use your information to provide you with information about M&S Bank companies' products and services, and also products and services from our partners and other relevant third parties. This includes marketing by post, email, telephone, text, secure messages or advertising to you and other people online and on social media. The lawful basis for this is our legitimate interest. We may need your consent to communicate by certain channels and we'll always make sure we get this where we need

to. You 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.

- Protecting our legal rights: we may need to use your information to protect our legal rights, for example in the case of defending or for the protection of legal rights and interests (for example, 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 acquisition. This may be in connection with action taken against you or other persons, for example, 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.