Raphaels Bank
Bankers since 1787

Dear customer,

We are making it easier for you to find out how we handle your information

The General Data Protection Regulation was introduced on 25th May 2018. As a result, we are publishing a new Privacy Notice to make it easier for you to find out how we (Raphaels Bank) use and protect your information. The new Privacy Notice will provide you with additional details such as:

- Your increased rights in relation to the information we hold about you
- How we keep your personal information secure
- The types of personal information Raphaels Bank collects about you and how we collect and use it
- The legal grounds for how we use your personal information

The new Privacy Notice replaces the Personal Information section in your prepaid card terms and conditions. You can also view a copy online at the website address set out in your prepaid card terms and conditions.

We will keep you up to date

The Privacy Notice makes sure that we continue to comply with privacy law and regulation. If we make changes to the Privacy Notice in the future, we will let you know.

We are here to help

If you have any questions or would like some help, please go to www.raphaelsbank.com/about/contact-us or email us at paymentservices@raphael.co.uk.

Yours faithfully

Raphaels Bank

Payment Services Privacy Notice

Intro

In providing you our services and products, we receive, use and share personal data about you. The information contained in this privacy notice tells you how your personal data is collected, used and shared by **R. Raphael & Sons plc** ('Raphaels Bank', 'we', 'us' or 'our'). You can find out more about us at our website: www.raphaelsbank.com

Raphaels Bank is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Raphaels Bank is registered in England and Wales under registration number 1288938, and our registered office is at 19-21 Shaftesbury Avenue, London, W1D 7ED.

Your information will also be held, used and shared on our behalf by our programme manager **Mastercard Prepaid Management Services (MPMS)** Cygnet Park Hampton Peterborough PE7 8FJ United Kingdom and its subsidiaries. You can find out more about our programme manager at: Website: **https://www.mastercard.co.uk/en-gb/issuers/products-and-solutions/grow-manage-your-business/payment-innovations/processing-solutions.html**

This privacy notice covers the following:

1. What information we collect and where we get it from

2. What are the legal grounds we rely on to process your data?

3. Legitimate Interest

4. How we use your information and with whom do we share your information

5. Profiling

6. Safeguarding your personal data

7. International Transfers

8. How long do we hold your information for?

9. Your legal rights

10. Updates to this privacy notice

11. How to contact us, complain or request access to your personal data

1. What information we collect and where we get it from

We use a lot of different types of personal data and obtain it from a number of different sources. We either receive your personal data from you directly, financial instructions, distributors and other services providers or generate the data ourselves (for example, during the provision of our services we generate transactional data about you). The type of information may include the following:

Type of personal data	Description	Purpose for processing it	How long we store it for
Your identity and contact details and those of other joint applicants	Your full name, and other information that may be obtained to verify your identity, residential address, mobile telephone and/or landline number, e-mail address and those of other applicants or secondary card holders.	Providing you with a financial service and notifying you about any changes to the product or the provision of the service; Prevention of financial crime and fraud against you; Sending you direct marketing if you have consented to receiving it.	Data about your identity will be stored for up to five years after the termination of the contract, unless we are legally obliged to keep them for longer. Any personal data held only for marketing purposes will be deleted as soon as consent is withdrawn by you.
Date of birth and / or age	Your date of birth or age.	Ensuring that you are eligible to apply for the service; Prevention of financial crime and fraud against you.	Data about your age or date of birth will be stored for up to five years after the termination of the contract, unless we are legally obliged to keep them for longer.
Financial identifiers	Your card and/or account details such as account number and sort code we ascribe to you and identifiers of the parties you are receiving money from or are sending money to.	Providing you with a financial service, including resolution of your requests for information, disputes and complaints, compliance with industry and regulatory requirements and prevention of financial crime and fraud against you.	Financial identifiers data will be stored for up to six years after the final transaction, unless we are legally obliged to keep them for longer.
Your economic position	Your income and in some occasions the funds you use to load our product and whether you or a close family member hold an important public office or you are a close business associate of a person that holds an important public office.	Prevention of financial crime and fraud against you.	Data about your financial position will be stored for up to five years after the contract has been terminated, unless we are legally obliged to keep it for longer.
Information concerning the product	The date when you applied for and/or obtained the product, any shared access to your product, the purpose for obtaining the product and any communication we may have with you concerning the product, including your complaints about our product and/or service.	Providing you with a financial product or service and prevention of financial crime and fraud against you.	Data about the payment product will be stored for up to five years after the contract has been terminated, unless we are legally obliged to keep it for longer. Information specific to a complaint will be stored for up to three years from the date complaint was received. Data required for preventing financial crime will be stored for up to six years after the final transaction, once the contract has been terminated, unless we are legally obliged to keep them for longer.

Type of personal data	Description	Purpose for processing it	How long we store it for
Usage data	The location and times where the product is used. Where the product offers an online portal or other online services we will also obtain technical data about you, including internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.	Providing you with a financial product or service, prevention of financial crime and fraud against you.	The data about your usage of the product will be stored for up to six years after the final transaction, unless we are legally obliged to keep it for longer.
Your personal situation (where you choose to share it with us)	Your personal data relating to difficult circumstances or a medical condition.	Providing you with a tailored service in line with your personal needs.	Data about your personal situation will be stored for up to five years after the contract has been terminated, unless you instruct us to erase this information at any point before the termination of the contract.

2. What are the legal grounds we rely on to process your data?

We can only use your personal information where it falls into one or more categories. Raphaels Bank relies on a few different legal grounds to process your data:

- It is necessary to the fulfilment of a contract we have with you;
- We have a legal or regulatory obligation to do so;
- It is our legitimate interest to do so and it is not against your rights;
- You have provided your consent to the processing.

Further information on the specific legal ground used for processing can be found in Section 4 'How we use your information'.

3. Legitimate Interest

The UK's data protection law allows the use of personal data where its purpose is legitimate and is not outweighed by the interests, fundamental rights or freedoms of data subjects.

The law calls this the 'Legitimate Interests' ground for processing personal data. Our use of this personal data is subject to an extensive framework of safeguards that help make sure that people's rights are protected. These include the information given to people about how their personal data will be used and how they can exercise their rights to obtain their personal data, have it corrected or restricted, object to it being processed, and complain if they are dissatisfied. These safeguards help sustain a fair and appropriate balance so our activities do not override the interests, fundamental rights and freedoms of data subjects.

If you think a decision is unfairly balanced in our favour you have the right to object to processing or to the restriction of processing. To find out where we rely on the legal grounds of 'legitimate interest' view Section 4 e) 'Chargebacks'.

4. How we use your information and with whom do we share your information.

Your personal data will be used to perform the services we provide to you. We also process your personal data to fulfil our regulatory and legal obligations as a regulated and authorised entity. In particular, we may use your personal data for:

a) Providing you with a financial service

In order to provide you with a financial service as detailed in our Terms and Conditions, we will collect your contact name, residential address and means to contact you (such as your e-mail address, mobile telephone number etc.). We may assign a customer reference number or another unique identifier to you in order to reduce the risk of disclosing your information to unauthorised third parties. We may also track technical data about you and the device you are using when you use an online portal to authorise a transaction, manage your online portal settings or view your available balance.

Who we share your data with for the provision of a financial service:

We use outsourced third-party providers such as:

- programme manager who assist us in providing the financial service to you MPMS Cygnet Park Hampton Peterborough PE7 8FJ United Kingdom,
- processors who assist us in processing the transaction data to the financial institutions you are transacting with - Mastercard Payment Transaction Services (MPTS) 2000 Purchase Street, Purchase, NY 10577 U.S.A;
- card bureaus who produce the payment card we issue to you - Gemalto - 1st Floor, GPS House, 215 great Portland Street, W1W 5PN;
- card services who will assist you with any questions and complaints about the financial service we are offering Telus, PO Box 7575 Vancouver, BC V6B 8N9; and
- Your card and account payment scheme – Mastercard, 10 Upper Bank Street, Canary Wharf, London, United Kingdom E14 5NP.

The legal grounds on which we rely for such data processing is fulfilment of a contract.

b) Preventing Financial Crime

We have legal and regulatory obligations to ensure that the financial services we offer are not exploited for illegal ends. In order to comply with our legal and regulatory obligation we have to ensure the information we receive about you which we rely on to provide you our products and services is accurate. As part of our duties we use your personal data to verify information e.g.

- your identity and that of the persons and companies you are transacting with,
- date of birth and residence,
- your economic situation and the economic means you use to load and spend using our payment instrument(s),
- the purpose(s) for which you are using the product.

We match your identification data against a database of Politically Exposed Persons (PEPs), sanctioned individuals and people of interest. We do this in order to identify whether you are on a list of sanctioned individuals, hold an important public office, are closely related to a person holding an important public position or are a business associate of a person holding an important public position.

We will also review your transaction history and any communication you may have with us or our outsourced service providers and will conduct profiling with your identity information, your transaction history and any communication in order to detect any form of financial crime. We use this data exclusively for detecting and preventing criminal activity (e.g., fraud, money laundering, terrorist financing, bribery etc.).

Who we share your data with for the prevention of financial crime:

We use:

- programme manager – MPMS, Cygnet Park Hampton Peterborough PE7 8FJ United Kingdom,
- Customer Due Diligence provider Netreveal - Surrey Research Park Waterside House, 170 Priestley Rd, Guildford GU2 7RQ, RDC - support@rdc.com and GB Group - 01244 657333
- Processor - Mastercard Payment Transaction Services (MPTS) 2000 Purchase Street, Purchase, NY 10577 U.S.A,
- PEPs and sanction-screening provider - Netreveal - Surrey Research Park Waterside House, 170 Priestley Rd, Guildford GU2 7RQ, RDC - support@rdc.com and GB Group - 01244 657333

Where we suspect that your payment instrument(s) has/have been used to conduct financial crime we have a legal obligation to report our suspicion to law enforcement agencies. In such instances, we are not permitted to inform you about such data sharing.

The legal grounds on which we rely for such data processing are legal and regulatory obligations we need to comply with.

c) Public Bodies and Law Enforcement

The police and other law enforcement agencies, as well as public bodies like local and central authorities and our regulators, can request us to supply them with personal data. This can be for a range of purposes such as preventing or detecting crime, fraud, apprehending or prosecuting offenders, assessing or collecting tax, investigating complaints or assessing how well a particular industry sector is working.

The legal grounds on which we rely for such data processing is legal and regulatory obligations we need to comply with.

d) Complaints

We are a credit institution regulated in the UK. As part of our legal obligations under the Financial Services and Markets Act we are obliged to handle any complaints you may have about our products and services. In instances where we are unable to resolve your complaint to your satisfaction you may raise your concern with the Financial Ombudsman Service (FOS) whose website can be found here: http://www.financial-ombudsman.org.uk/. In such instances the FOS may contact us to obtain evidence from us on the disputed particulars which will contain your personal data relating to your complaint. In order to help the FOS to resolve your complaint we are then required to disclose relevant details of the case to them so they can undertake their own review.

The legal grounds on which we rely for such data processing is legal and regulatory obligations we need to comply with.

For further information about our complaints procedure please email Prepaidmgmt_Globalcomplaints@mastercard.com we can provide you with a copy of this procedure if you request a copy in writing.

e) Chargebacks

If we have a legal claim against you in situations where you have accrued a negative balance on your card or account and you do not rectify it we may pursue the legal claim in the courts.

The legal grounds on which we rely for such data processing is legitimate interest.

f) Direct marketing

We may contact you by email and/or push notification, with information about related services and offers which we believe will be of interest to you.

You may opt out from receiving marketing communications by clicking on the unsubscribe link contained in any such communications. You can in addition change your preferences at any time by calling us, writing to us, or by updating them online where you can advise us that you no longer wish to receive any marketing material.

The legal ground on which we rely for such data processing is legitimate interest.

Please view the column 'How long we store it for' in the table in Section 1 to find out how long we hold specific sets of personal data for.

g) Vulnerable persons

Our customer service may offer you a better tailored service if you authorise our customer service team to establish with you and record whether you are suffering from any condition or circumstance that may impede your communications with us. In those instances we might be able to provide you with information more appropriately designed to improve your understanding of our products and services. If you wish that we should record specific information about difficult circumstances or a condition impeding your communications with us, please contact us:

- Stating your condition.
- List any information about the means of communication (that we can reasonably accommodate) that you would prefer as the means by which we communicate with you.

If you choose to consent to us recording this information you can contact us at any time to request us to stop processing or erase your data relating to your condition or difficult circumstances. If you do not do so we will delete this information as soon as you have redeemed all of your remaining funds with us.

The legal grounds on which we rely for such data processing is your explicit consent.

Raphaels Bank will store this data, until you withdraw your consent.

h) Audits and regulatory oversight

We are legally obliged to carry out audits in order to ensure our activities meet relevant financial services regulation like the Payment Services Regulations 2017 and regulation associated with it such as the Money Laundering Regulations 2017. As part of any audit our auditors may review some customer files for the purpose of ensuring that some or all areas of compliance of how we provide a product or service to you have been met. When this happens your customer file might be reviewed as part of a sample of files in order to review whether we handled you in an appropriate manner.

In some instances we use external auditors in order to review our compliance and your data may form part of such a review.

Raphaels Bank is regulated by the Financial Conduct Authority (FCA) for providing financial services and by the Information Commissioner's Office (ICO) for the purpose of data protection. Both may carry out audits on aspects of Raphaels Bank's quality and relevant compliance when providing their services and products.

The legal grounds on which we rely for such data processing is legal and regulatory obligations we need to comply with.

5. Profiling

We carry out profiling in three different scenarios:

- The prevention of financial crime;
- Safeguarding your online portal against fraudulent access by unauthorised parties;
- Marketing.

When we are trying to prevent financial crime we will combine your personal data concerning identity, economic situation, purpose for taking up the product and your economic activity (in some cases this includes formal documentation evidencing where you obtained the funds you wish to spend with us) with the financial information we gather when you perform transactions and the communication you engage in with our customer service team. We do so in order to identify any suspicious behaviour that could indicate your participation in criminal activities or third parties using your data to commit fraud. Where we suspect any criminal activity we are legally obliged to report it to law enforcement agencies.

When we process your data to protect your online portal against unauthorised use by third parties we will combine the technical information you submit as an electronic "footprint" with the actions you usually take when logging into the portal. This allows us to identify any

unexpected use which may indicate unauthorised access. In instances where we suspect unauthorised access we may block the portal and contact you as soon as possible, unless we are not permitted to do so by law.

If you have consented to receive marketing material from us we may analyse your spending behaviour in order to send targeted marketing to you.

If you have concerns regarding the manner in which we conduct profiling, you would need to contact us via the contact information in the Section 12 'How to contact us, complain or request access to your personal data'.

6. Safeguarding your personal data

We take the protection of personal data very seriously and we will maintain appropriate safeguards to ensure the security, integrity and privacy of your information. We restrict access to your personal data to those employees, service suppliers and sub-contractors who need to know that information to provide products or services to you. Those persons are also subject to a duty of confidentiality.

7. International Transfers

We are in the United Kingdom. In certain circumstances, we will need to send or allow access to personal data from elsewhere in the world. This might be the case, for example, when a processor or agency is based overseas or uses overseas data centres.

While countries in the European Economic Area all ensure a high standard of data protection law, some parts of the world may not provide the same level of legal protection when it comes to personal data. As a result, when we do send personal data overseas we will make sure suitable safeguards are in place in accordance with European data protection requirements:

- Sending the data to a country that is approved by the European authorities as having a suitably high standard of data protection law. A full list of the approved countries outside the EU can be found at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
- Putting in place a contract with the recipient containing terms approved by the European authorities as providing a suitable level of protection. Read more about this on the European Commission Justice website https://ec.europa.eu/info/law/law-topic/data-protection_en
- Sending the data to an organisation which is a member of a scheme that's been approved by the European authorities as providing a suitable level of protection. One example is the Privacy Shield scheme agreed between the European and US authorities.
- Binding Corporate Rules which allow multinational corporations, international organizations, and groups of companies to make intra-organizational transfers of personal data across borders in compliance with EU Data Protection Law. For more information on binding corporate, we refer you to the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/

8. How long do we hold your information for?

We will retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of any legal, accounting or reporting requirements.

Whilst you continue to be our customer, we will keep a record of your personal information to ensure that we provide you with the best service possible and where we are required to keep your personal information to meet our legal and regulatory obligations. Please view the column 'How long we store it for' in the table in Section 1 to find out how long we hold specific sets of personal data for.

We will delete your personal data or keep it in a form that does not permit identifying you when this information is no longer necessary for the purposes for which we process it, or when you request their deletion, unless we are required by law to keep the information for a longer period.

9. Your legal rights

Subject to applicable law, you have the right to:

Access your personal data, rectify it, restrict or object to its processing, or request its deletion:

a) Access to your data

You may request access to your personal data (commonly known as a 'data subject access request'), to update and correct inaccuracies in your personal data, to have the information anonymised or deleted, as appropriate. This enables you to receive a copy of the personal data we hold and to check that we are lawfully processing it.

b) Objection to processing

You have the right to lodge an objection about the processing of your personal data by us. However, you should know that under the General Data Protection Regulation, we will not be able to stop processing your data in all instances, We can stop processing your data as explained under Section 2 'What are the legal grounds we rely on to process your data'.

In many cases - particularly where personal data is being processed for activities such as prevention of fraud and anti-money laundering, supporting responsible lending and suspicious activities reporting - we are not permitted by law to stop processing or delete personal data immediately or prior to five years after the end of our business relationship.

c) Restriction to processing your data

You have the right to request restriction of processing your data. We can restrict the processing of specific data items in situations where you believe that the data we hold about you is inaccurate, for example when you have moved house and we still hold your previous residential address. In such cases we may request formal documentation supporting any requested amendments to your data.

In some circumstances, you can ask us to restrict how we use your personal data. Your rights are set out at Article 18 of the General Data Protection Regulations www.eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016R0679. You cannot enforce this right in all circumstances, and your personal data may still be processed where certain grounds exist. This is:

- where we have to follow a statutory obligation (you can find relevant areas where we have to comply with statutory obligation in Section 2 'What are the legal grounds we rely on to process your data');
- For the establishment, exercise, or defence of legal claims;
- For the protection of the rights of another natural or legal person;
- For reasons of important public interest.

Only one of these grounds needs to be demonstrated to continue data processing. Please see Section 2 'What are the legal grounds we rely on to process your data' for a description of the legal grounds upon which we rely for processing of personal data.

We will consider and respond to requests we receive, including assessing the applicability of these exemptions. However, it is important to note that in many circumstances we will be unable to provide you with our services without using your personal data. If you want to object to the use of or restrict how we use your personal data, please use the contact details in Section 12 'How to contact us complain or request access to your personal data'.

d) Rectification of personal data

1. In some instances, we might hold outdated information about you like a mobile telephone number that you no longer use. You have the right to ask us to change this information. In some instances, we will need to ensure that the new information is correct and may request documents from you to verify its accurateness.

2. Request transfer of your personal data to you or a third party. We will provide to you, or to a third party that you have chosen, your personal data in a structured, commonly used, machine-readable format. Please note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

3. Withdraw consent at any time where we are relying on consent to process your personal data at any time and free of charge. However this will not affect the lawfulness of any processing carried out before you withdraw consent.

4. Right to lodge a complaint with your supervisory authority.

10. Updates to this privacy notice

We may update this notice from time to time by publishing a new version on our Programme Manager's website. We will endeavour to contact you regarding changes to this privacy notice, where possible and appropriate. However, you may also wish to check this page occasionally to ensure you are up to date and/or aware of any changes to this Privacy Notice.

11. How to contact us, complain or request access to your personal data

For general personal data enquiries, please contact Card Services at **Mastercard Prepaid Management Services (MPMS)** Cygnet Park Hampton Peterborough PE7 8FJ

If you would like to exercise one of your rights under GDPR or escalate an issue, please contact our Data Protection Officer:

To make a request by email: dataprotectionofficer@raphael.co.uk

To make a request by post: Data Protection Officer, Raphaels Bank, 19-21 Shaftesbury Avenue, London, W1D 7ED

Please let us know if you have any feedback or are dissatisfied with how we have used your personal data. You can contact us using the above contact details.

You also have the right to complain to the Information Commissioner's Office ("ICO"), the UK Supervisory authority for data protection issues at https://ico.org.uk/concerns/. However, we would appreciate the opportunity to deal with your concerns before you approach the ICO so please contact us in the first instance.

Head Office

Raphaels Bank is a registered trading name for R. Raphael & Sons plc, 19-21 Shaftesbury Avenue, London, W1D 7ED

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority,

Registration No. 161302