PRIVACY POLICY

Last Updated: March 9, 2026

1. Scope

"We", "our", "us", or "MNEE Pay" refers to the entity listed at the end of this privacy notice with which you or your organization have a relationship.

This privacy notice describes how MNEE Pay collects, use, and process personal information in relation to your use of our services supplied through the MNEE Pay platform ("Platform"), website ("Site") and applications ("Apps") (together, the "Services" , which includes digital asset services, money transmission, and fiat currency services, provided in compliance with our federal registration as a Money Services Business (MSB) and various State Money Transmitter Licenses (MTLs).

Undefined capitalized terms used in this privacy notice can be found in the applicable agreement or terms of use for the Services (each, an "Agreement"). If you are a Customer, Authorized Customer (in this privacy notice each, a "Customer") of MNEE Pay Services, this privacy notice applies to you as well as any Agreement or other disclosure that may be provided to you by us.

Our privacy notice is applicable to all Customers who access or utilize our Services and covers personal data processing activities carried out by us in our Services.

MNEE Pay may offer or facilitate certain fiat banking or payment features (including, as applicable, bank accounts, debit cards, ACH, and related services) through one or more U.S. financial institution partners (each, a "Bank Partner"). Where you use a feature provided by a Bank Partner, MNEE Pay may collect and process certain personal information on behalf of the Bank Partner to enable the provision of the Bank Partner service. In those cases, the Bank Partner's own privacy notice and applicable U.S. federal financial privacy laws, including the Gramm-Leach-Bliley Act ("GLBA"), may apply to that information.

Certain U.S. state privacy laws provide exemptions for personal information subject to GLBA; where applicable, those exemptions may limit the scope of

state-law rights for data processed under GLBA-governed banking services. Nothing in this Privacy Policy limits your rights under applicable law.

2. Processing your personal data (Controller)

The personal data we process and our role under data protection laws can vary depending on how you interact with MNEE Pay. For example, you may be: (i) an individual customer; (ii) an authorized user of an account held by a business customer (e.g., a company administrator, employee, or cardholder where business accounts and/or card services are offered); (iii) a beneficial owner, director, officer, or other control person of a business customer (for KYB and regulatory purposes); or (iv) a recipient or counterparty in connection with a transaction.

Where MNEE Pay determines the purposes and means of processing your personal data, MNEE Pay acts as a controller. In certain business/corporate scenarios (e.g., where a company provides employee data for account administration, expense management, or card issuance), that company may act as a separate controller for its own processing, and MNEE Pay acts as a controller for MNEE Pay's own regulated service processing.

3. Protection and storing of your personal data

MNEE Pay is committed to implementing security measures that are reasonably expected to safeguard Customer's personal data from destruction, loss, modification, or any other unauthorized processing. Some of the security measures that MNEE Pay will implement include, without limitation:

3.1 Encryption. We employ industry-standard encryption protocols to secure the transmission and storage of personal data. This encryption helps prevent unauthorized access and ensures the confidentiality and integrity of the information.

3.2 Access Controls. Access controls are in place to restrict access to personal data to only those employees or authorized personnel who require it for legitimate purposes. These individuals are bound by strict confidentiality obligations and are aware of the importance of protecting personal data.

3.3 Self Help. Customers are encouraged to take their own precautions, such as using strong and unique passwords and regularly updating their devices and software, to further enhance the security of their personal data. MNEE Pay will never ask you to disclose your passwords, PINs, or one-time passcodes via email, SMS, or phone. You are responsible for keeping

credentials and security codes confidential and for promptly notifying us of suspected compromise.

3.4 Private IP. Customer data is stored on a server with no public IP address. Only specific servers can contact this server in a separate private network.

3.5 Connections. SSH connection to public servers can only be done from the (virtual) private network of MNEE Pay.

3.6 Passwords. Customer passwords and private keys are always hashed (not stored in plain text). Customer data is stored in a database with access control and all user data (which is inside the database) is encrypted at rest.

4. Information and data collected

At MNEE Pay, we value transparency and strive to provide clarity on our data collection and processing practices. The table below presents an overview of the data we collect, its source, category, a brief description, and the lawful basis for processing.

Please keep in mind that the specific data we collect may vary depending on the MNEE Pay Service you are using. Therefore, the table provides a comprehensive list but does not limit the data we collect or imply that we collect this data in all instances.

We collect data through various methods, such as customer registration, Transactions, program participation, industry events, and customer service communications. Where we collect personal data to administer our contract with you or to comply with legal/regulatory obligations, providing such data is mandatory and we may not be able to provide the Services without it. In other cases, providing personal data is optional, but this may affect your ability to access certain features or functionalities where the data is needed for those purposes.

Our services are not directed to children and are intended for individuals who are 18 or older. We do not knowingly collect personal information from individuals under 18. If we learn we have collected such information, we will take steps to delete it consistent with applicable law.

Source	Category	Description	Lawfulness of processing

1. Information provided by Customer*	Basic Information	**Identity Information:** First Name & Last Name, gender, username, title, Nationality/Citizenship, Country of residence, job title/employment information and proof of residency	Performance of contract
		Contact Information: Billing Address, Email address, Phone number. We may use address auto-complete/autofill functionality provided by third parties to help you populate address fields during onboarding; this may involve limited address-related data being processed by that provider.	Performance of contract & communicate with you
		ID number (when applicable).	Performance of contract
		Tax identification number of every tax residency, all jurisdiction(s) (countries) of tax residence	Performance of contract
	Required by Law in the context of KYC or AML obligations	Date and place of birth.	compliance with a legal obligation

	Copy of user's identity card or passport Biometric information (where used): Selfie images/videos, liveness checks, facial scan templates/biometric identifiers derived from images/videos, and related metadata used to verify identity, authenticate access, and prevent fraud.	compliance with a legal obligation
Provided by Customer	**Government identifiers:** Social Security number (where required), driver's license/passport or other government ID numbers, tax identification numbers, and related verification attributes collected for onboarding, fraud prevention, compliance, and (where applicable) Bank Partner services.	Performance of contract; legitimate interests; compliance with a legal obligation (as applicable).
	Financial Information such as: bank account details, payment card details, and/or cryptocurrency wallet address(es), balances and transactions, Income, details about source of funds, trading and investment experience, net worth/asset verification statements.	Performance of contract; legitimate interests; compliance with a legal obligation (as applicable).
	Customer Support and Communications Data: Records of communications with us	Performance of contract; legitimate interests; compliance

		(including emails, chats, tickets, and - where permitted - recordings and/or transcripts of phone calls) for training, quality assurance, dispute handling, and compliance recordkeeping.	with a legal obligation (as applicable).
		Communications preferences: may include your preferences in receiving communications/marketing from us and our third parties.	Consent is given
2. Information Collected Automatically	App, browser, and device information	**Technical Data:** may include 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, other technology on the devices you use to access the Sites and Services, device language, device type, whether the device uses a virtual private network (VPN), and unique device identifiers (such as device or advertising identifiers where available, and similar identifiers depending on device settings).	Performance of contract & ensure functionality
	Service Usage	**Transaction Data:** may include details of transactions and activity	Performance of contract & ensure functionality

Information	performed through the Services (including deposits/withdrawals, conversions, transfers, and card-related transactions where applicable), such as date/time, amount, currency, exchange rate, beneficiary/sender details, merchant or ATM information (including location where available), transaction messages/notes, IP address or device/network indicators associated with initiating or receiving the transaction, and the payment method or device used to initiate the transaction.	
	Activity information: Information about what you view or click on while visiting our Sites and Apps and how you use our Services.	Performance of contract & ensure functionality
	Profile data: may include your username and password, purchases or orders made by you, your digital asset transaction history / account activity, your preferences, feedback, and survey responses.	Communicate with You & ensure functionality
	Diagnostic and Troubleshooting Information: how our	Performance of contract & ensure functionality

		Services are performing when you use them, i.e. service-related diagnostic and performance information, including timestamps, crash data, website performance logs, and error messages or reports.	
	Information from cookies and similar technologies	We and our service providers use cookies, pixels, SDKs, web beacons, and similar technologies to operate our Services, remember preferences, help with sign-in and security, measure performance, understand usage, and personalize content. You can manage cookies through your browser settings and, where available, through in-product privacy controls.	See our cookie policy available here https://rockwallet.com/cookie-policy or elsewhere on our website.
3. Information we obtain from Affiliates and third parties	RW Group of Companies ("Affiliates")	We may obtain information about you, such as basic Information, transaction information and product usage from our Affiliates as a normal part of conducting business.	Performance of contract & ensure functionality
	Public Database Information	We may obtain information about you from public databases, such as the United Nations Sanctions List, US ITA Consolidated	compliance with a legal obligation

	Screening List, OFAC, and the SEC EDGAR. We may also obtain publicly available information from media reports, online registers/directories, or public social media content to support KYB/KYC, sanctions screening, fraud prevention, and enhanced due diligence.	
Fraud risk ratings / sanctions status / verification results	We may receive fraud risk ratings, sanctions/PEP/adverse mediascreening status, transaction monitoring alerts, and verification results from identity verification, anti-fraud, AML, and sanctions screening providers.	compliance with a legal obligation
Blockchain Data	We may analyze public blockchain data, including timestamps of transactions or events, transaction IDs, digital signatures, transaction amounts, and wallet addresses.	Ensure functionality
Information from our Marketing and Advertising	We receive information such as your name and contact information from our marketing partners, including in some instances what marketing content you viewed or the actions you take on our Sites. If you communicate with or	Marketing

Partners	interact with our pages or brand on social media, we may receive information about your interaction from the relevant platform and/or social media analytics providers. Our emails may include a “click-through URL” that routes through our systems before taking you to the destination webpage. We use this information to understand engagement with our communications (for example, which topics are most relevant) and to measure effectiveness of customer notices and updates. If you prefer not to be tracked in this way, avoid clicking links in marketing emails.	
Information from Analytics Providers	We receive information about your Site usage, interactions, age group, and survey responses (including prior to account creation, in some cases).	Marketing
Retail Merchant Information	If you use your account to conduct a transaction with a third-party merchant, the merchant may provide us with data about you, such as your name and contact details, and your transaction with that merchant.	Performance of contract

Research and In-App Survey Information	We use third party service providers to conduct in-app surveys to better understand our customers' experience and improve our Services. The information we receive from our research partners is pseudonymous.	Improve services

*For entities, we may collect some of this information for individual members such as beneficial owners, directors, etc., as applicable.

We may also collect, use, and share aggregated data, such as statistical or demographic data, for various purposes. Aggregated data is derived from your personal data but is considered non-personal data under the law, as it does not directly or indirectly disclose your identity. For example, we may analyze your Service Usage Information in an aggregated form to determine the percentage of users accessing specific features on our Sites. However, if we combine or link aggregated data with your personal data in a way that allows us to identify you directly or indirectly, we will treat the combined data as personal data and handle it in accordance with this privacy notice. Our approach to handling aggregated data aligns with industry-standard privacy practices.

5. Purposes of the collection and processing

MNEE Pay can process personal data for (one of or several) the following purposes, based on one or more legal grounds:

5.1. Performance of contract. Customer information will be utilized for account creation and identity verification to provide our Services. It may also be used for Services related to Transactions and for technical support, issue resolution, and ensuring the safety and quality of the services.

5.2. Ensure Functionality. To ensure the proper functioning of the Services, as well as the provision of ordered Services, the information listed above may be processed.

5.3. Communicate with You. We utilize the information to address your inquiries, fulfill your requests, and send crucial notifications. This encompasses activities such as sending periodic emails concerning company updates, policy changes, product/service enhancements, or press releases.

5.4. Marketing. We use the information we have about you to market our services. This includes, for example, sending you email communications about products, offerings, events, competitions, surveys, and webinars or customized offers or materials. Our marketing efforts are aligned with your communication preferences, and you always retain the right to unsubscribe. We may send marketing communications through channels such as email, SMS/text, in-app messages, push notifications, and phone calls, subject to your preferences and applicable law. We may also use pixels or similar technologies in our emails to understand delivery, opens, clicks, and campaign effectiveness, and to improve our communications.

5.5. Improve Services. We use the information we have about you to improve our services. This includes, for example, identifying usage trends, developing data analysis, determining the effectiveness of our promotional campaigns, evaluating our business performance, researching, demonstrating, developing, and improving our products and services, and ensuring quality control.

5.6. Comply with Laws. We use the information we have about you to comply with applicable laws, regulations, and contractual obligations. This includes, for example, “know your customer” (KYC), “know your business” (KYB) obligations, conducting compliance and/or security checks, audits, or assessments, and any related reporting obligations.

5.7. Protect assets, prevent, detect, and investigate fraud, unlawful or criminal activities in relation to our services. We use the information we have about you to protect our rights and interests, ensure the security of our assets, systems, and networks, prevent, detect, and investigate fraud, unlawful or criminal activities in relation to our services, and enforce our terms and conditions. This includes proactive measures such as Account Takeover (ATO) prevention and support. Note: We may use automated processes (including risk scoring and fraud/AML screening) to help detect fraud, comply with applicable laws, and protect our services and customers. Where required by applicable law, you may have the right to request meaningful information about such processing and/or to request a human review of an automated decision that produces legal or similarly significant effects, and to contest the decision.

5.8. Banking, payment, and card features (where applicable). Where we offer or facilitate fiat banking, payment, or card services (including through Bank Partners), we may use personal data to: (i) establish and manage linked bank accounts and cards; (ii) facilitate deposits, withdrawals, ACH and card transactions; (iii) administer chargebacks, disputes, and compliance

monitoring; (iv) provide transaction notifications and statements; and (v) meet Bank Partner operational and compliance requirements.

5.9. Quality assurance, training, and service improvement. We may use customer support interactions, including call recordings where permitted, to train personnel, monitor quality, troubleshoot, and improve the Services.

5.10. Determine legal eligibility and suitability. To comply with applicable financial laws and regulations that require us to ensure your suitability and legal eligibility for certain regulated financial products, account activities, or fiat services provided in partnership with ourpartners.

5.11. Other Purposes that require your consent. Except as required by Applicable Law, we may share or disclose your information only if you provide your prior consent.

6. Third-party access to Customer's personal data

We do not share personal information with companies, outside organizations, individuals, or other recipients unless one of the following circumstances apply:

6.1. Legal, Regulatory, Safety, and Compliance Purposes. In certain situations, we may be required to share your information as required by law. These situations may include but are not limited to complying with a subpoena or other legal process requests; protecting your rights; protecting your safety or the safety of others; investigating fraud; and responding to a government request. This includes, but is not limited to, mandatory requests from FinCEN (as a registered MSB), state financial regulators (for MTL compliance), the IRS, or other regulatory bodies as required for our ongoing compliance.

6.2. Sharing with Service Providers and Third Parties. MNEE Pay may disclose your information to third-party service providers who assist us in managing the Services. These providers may include IT service providers, data storage providers, identity verification service providers, payment processors, telecommunications technology providers (for SMS/2FA), CTF/AML service providers (for transaction monitoring), cloud service providers, and marketing service providers. However, we ensure that these providers are only allowed to use your personal information for the sole purpose of providing their services to us and not for their own promotional purposes. Your personal data may be stored within their systems, but we require them to uphold the confidentiality of your information and comply with all privacy and data protection laws. Rest assured; we do not sell your

personal information to third parties. We take steps to assess service providers before engagement and to require appropriate contractual safeguards, including confidentiality, security measures, and limitations on processing consistent with the services provided.

6.3. Plaid. For Services provided by MNEE Pay LLC, to ensure fraud prevention and mitigation, we utilize Plaid, Inc. as a service provider for third-party identity verification. Plaid, Inc. performs bank account verification, balance confirmation, and transaction history review to approve transactions. Your personal and financial information is handled in compliance with Plaid's privacy notice, which can be accessed at https://plaid.com/legal/#privacy-policy. By utilizing our services, you authorize MNEE Pay and Plaid, Inc. to access and transmit your personal and financial information from your bank according to such privacy policy.

6.4. MNEE Pay Affiliates. We may share your information within MNEE Pay Affiliates for various purposes, including providing you with our services, preventing fraud, conducting identity verifications, complying with the law, facilitating sales, mergers, acquisitions, or other liquidity events, and offering products and services to you. However, we do not share information about your creditworthiness with our Affiliates.

6.5. With your consent. We will share personal information with companies, outside organizations or individuals if we have your consent to do so.

6.6. Financial service partners. We may share your information as necessary to open and maintain your account, process transactions, issue cards, and comply with all applicable banking and Anti-Money Laundering regulations (e.g., GLBA, BSA etc.). The use of your data by our financial service partner is also governed by their separate privacy notice. We may share information with partner banks, card networks (e.g., Visa/Mastercard), processors, and other financial intermediaries as necessary to provide banking/payment/card features, handle disputes, and comply with law.

7. Data transfers

MNEE Pay may transfer your data to countries outside of the country from where you have accessed our Services. To ensure compliance with applicable data protection rules, we have implemented suitable technical, organizational, and contractual safeguards, including the use of Standard Contractual Clauses. When transferring personal data outside of the EEA or the UK, we adhere to lawful transfer mechanisms. If the European Commission has determined that a country provides an essentially equivalent standard of data protection as the EEA, we may rely on an

'adequacy decision' to facilitate the transfer of personal data. When transferring personal data from the EEA to the US, we may rely on standard contractual clauses.

8. Privacy when using digital assets and blockchains

We emphasize the protection and confidentiality of personal data when using digital assets. Public blockchains are designed to record transactions across networks of computer systems, and the use of digital assets are usually publicly recorded on these blockchains. It is important to note that public blockchains can undergo forensic analysis, which may potentially lead to the re-identification of individuals and the disclosure of personal data, particularly when combined with other data sources.

As a rule, cryptocurrency transactions are less private than fiat banking transactions because they occur on public blockchains.

As MNEE Pay does not have control over or operate these decentralized or third-party networks, we are unable to erase, modify, or alter personal data on such blockchains. We are committed to implementing appropriate safeguards and complying with applicable privacy laws and regulations to protect personal information within our control. However, we advise users to exercise caution and take necessary precautions when utilizing digital assets on public blockchains.

9. Your privacy rights and choices

Depending on where you live, you may be able to exercise certain privacy rights related to your personal information. For any of your privacy rights and choices referenced below, requests relating to your personal information can be made by logging into your account or by submitting a request via our Support Portal. We will assess and respond to requests in accordance with applicable law and may deny requests where an exemption applies (for example, where we must retain information to comply with legal obligations, prevent fraud, or protect the security of our services).

Right to access and portability: You may request that we provide you a copy of your personal information held by us by submitting a request via our Support Portal.

Right to rectification: You may request us to rectify or update any of your personal information held by MNEE Pay that is incomplete or inaccurate by logging in to your account and going to the Profile or My Account page. If you

cannot access or update particular information through those pages, then you can submit a request via our Support Portal.

Right to deletion/erasure: You may request to erase your personal information, subject to applicable law. If you close your MNEE Pay Account, we will retain or delete information associated with your account as determined by the regulatory requirements.

Right to withdraw your consent: To the extent the processing of your personal information is based on your consent, you may withdraw your consent at any time. The lawfulness of MNEE Pay's processing before you withdraw your consent will not be affected by such withdrawal.

Right to object to or restrict processing: You may have the right to restrict or object to us using or transferring your personal information based on our legitimate interests, in the public interest, or for direct marketing. We may continue to process your personal information where permitted or required by applicable law. You can opt-out of receiving marketing communications from MNEE Pay through your account settings or by submitting a request via our Support Portal.

Right to non-discrimination: We will not discriminate against you for exercising any of your rights provided to you under law.

Right to lodge a complaint: If you have a complaint about our practices with respect to your personal information, you can submit it via our Support Portal. We take all complaints seriously and will respond within a reasonable time.

To protect your privacy and security, we may take steps to verify your identity before complying with your request and we may decline your request if we are unable to verify your identity. Under certain US data privacy laws, you may also designate an authorized agent to make these requests on your behalf.

These rights are not absolute and may be denied: (a) when granting access or assisting portability would adversely affect the rights and freedoms of others; (b) to protect our rights and properties; (c) where the request is frivolous or vexatious; or (d) as otherwise permitted by law.

9.1. Data protection authorities.

If you have concerns about the processing of your personal data or believe that your rights under applicable data protection laws have been violated, you have the right to lodge a complaint with the relevant supervisory authority.

Depending on your state of residence and subject to applicable exemptions (including for data governed by GLBA), you may have certain rights regarding your personal information, such as: access, correction, deletion, portability, and the right to opt out of targeted advertising and certain disclosures that may be considered a “sale” or “share” under state law.

We will not discriminate against you for exercising your privacy rights. We may need to verify your identity before processing certain requests. If we deny a request, you may have the right to appeal our decision where required by law; appeal instructions will be provided in our response.

In the European Union, each member state has its own supervisory authority responsible for data protection matters. You can find the contact details of the supervisory authority in your country of residence or where the alleged violation occurred listed below or by searching your local governmental authority sites: https://edpb.europa.eu/about-edpb/board/members_en

We encourage you to contact the supervisory authority directly if you have any concerns or complaints regarding the processing of your personal data. However, we would appreciate the opportunity to address your concerns first, so please contact us and we will do our best to resolve any issues in a timely and satisfactory manner.

Please note that you are not obligated to contact us before lodging a complaint with the supervisory authority. You have the right to file a complaint directly with the supervisory authority at any time.

9.2. Contact us

If Customer intends to use any of its above-mentioned rights, please do so by directing Customer’s request to legal@rockwallet.com or by a letter to MNEE Pay (see address above). MNEE Pay cannot handle Customer’s request without proof of Customer’s identity and the applicable legislation may impose conditions on exercising the above rights.

MNEE Pay will request a copy of Customer’s identification document as proof that Customer are indeed concerned by the personal data and thus entitled to rights mentioned above.

MNEE Pay will use its best efforts to respond to Customer’s request without undue delay after receipt of Customer’s request.

Customer should bear in mind that MNEE Pay will not always be obliged to comply with a request for access, correction, removal or transfer, taking into

consideration the requirements related to the establishment, exercise or substantiation of a legal claim or the legitimate exercise of the right of freedom of expression and / or information.

10. Retention

We retain personal information for as long as needed or as permitted in light of the purpose(s) for which it was obtained and consistent with applicable law and, in any case, not less than five (5) years. The criteria used to determine our retention periods include:

• the length of time we have an ongoing relationship with you (for example, for as long as you have an account with us or keep using MNEE Pay),
• whether there is a legal obligation to which we are subject (for example, certain laws, such as anti-money laundering requirements including the Bank Secrecy Act (BSA) require us to keep records of your transactions for a certain period before we can delete them); and/or

whether retention is advisable considering our legal position or to protect the safety of individuals (such as regarding applicable statutes of limitations, litigation, or regulatory investigations).Where we (or our identity verification providers) process biometric information for identity verification or fraud prevention, we retain it only for as long as necessary for those purposes and to comply with legal obligations, and then delete or irreversibly de-identify it in accordance with our retention schedule and applicable law.

The processing of personal data under this Agreement is also subject to the provisions of the General Data Protection Regulation (GDPR) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=NL.

11. Legal rights of California residents

In addition to the legal rights provided above, in compliance with the California Privacy Act of 2018 (“CCPA”), residents of California may contact us at legal@rockwallet.com to request information on the types of personal information that we have disclosed during the preceding 12 months to third parties for their direct marketing purposes and the identities of those third parties.

For personal information collected by us during the preceding 12 months that is not otherwise subject to an exception pursuant to the CCPA, you have the right to access, correct and delete your personal information, and we hereby declare that we shall not discriminate against those who exercise those rights. Specifically, we shall not:

• deny you our services.
• charge you differently.
• provide you with a different level of quality of services; or
• suggest that you may receive a different price or rate for services or a different level or quality of services.

We further declare that we do not sell your personal information in our ordinary course of business and will never sell your personal information to third parties without your explicit consent.

If you seek to exercise CCPA access or deletion rights on behalf of another person, you must confirm that the person has authorized you to act as their agent under the CCPA by providing us with a completed, signed, and notarized CCPA Agent Authorization Form pursuant to California Probate Code Section 4000 to 4465. Please note that we may deny requests from agents who do not submit the relevant proof of authorization or agents we are unable to verify their identity.

Under the CCPA, you have the right, if certain parts of your personal information are part of a data security breach, to initiate a private cause of action.

You have the right to limit our use of sensitive personal information ("SPI") to what is necessary or reasonably expected of us to perform the Services. If we use SPI beyond what is necessary to provide the Services, we shall provide you notice of the additional purposes for our use of SPI and remind you of your right to request that we limit the use of the SPI.

SPI is a subset of personal information that reveals (i) your social security number, driver's license number, state identification card or passport number; (ii) your account log-in, financial account information, debit or credit card number in combination with any password or access code to grant access; (iii) your precise geolocation; (iv) your racial or ethnic origin, religious or philosophical beliefs, or union membership; (v) the content of your mail, email or text messages unless we are the intended recipient of said communications; and (vi) your genetic data.

12. Legal Rights of Vermont residents

We will not disclose information regarding your creditworthiness to our affiliates and will not disclose your personal information, financial information, credit report, or health information to non-affiliated third parties for marketing purposes, except as permitted by Vermont law or with your explicit consent.

Additional information concerning our privacy policies can be found at https://info.rockwallet.com/privacy-policy or call telephone number (302) 306-6201.

13. Legal Rights of Nevada residents

Company does not currently sell your covered information as those terms are defined under applicable Nevada law. You may still submit an opt-out request, and we will honor that request as required by Nevada law if Company were to engage in such a sale in the future. If you are a Nevada resident and would like to opt-out of the sale of your covered information, please submit your request to legal@rockwallet.com. Your request must include your full name and zip code. Please contact us from the email address you have used to interact with us, or else provide us with that email address in your Nevada Opt-Out request email. We may contact you via such email address as needed regarding this request. If you previously provided a phone number to us, including it in your Nevada Opt-Out request email will assist us in identifying you and processing your request. You may also be required to take reasonable steps as we determine from time to time in order to verify your identity and/or the authenticity of the request.

14. Updates to the privacy notice

We may update or modify this privacy notice from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. Any changes we make will be posted on this page with a revised "Last Updated" date. We encourage you to review this privacy notice periodically to stay informed about how we collect, use, and protect your personal data.

If we make any material changes to this privacy notice, we will provide notice by email (if we have your email address) or by posting a notice on our website prior to the change becoming effective. We will also seek your consent for any material changes to the extent required by applicable data protection laws.

Your continued use of our services after the effective date of any revised privacy notice constitutes your acceptance of the updated privacy notice. If you do not agree with the updated privacy notice, please refrain from using our services and contact us to deactivate your account, if applicable.

Please note that we are not responsible for the privacy practices of third-party websites or services that may be linked to or from our website. We recommend reviewing the privacy policies of those third parties directly.

If you have any questions or concerns about our privacy notice or practices, please contact us using the information provided in the "Contact Us" section above.

Need Help?

If you have any questions or need assistance, our support team is here for you at support@rockwallet.com.