OMNIBEK INC. DOING BUSINESS AS OMNIWIRE INC.

PRIVACY AND COOKIES POLICY

This Privacy and Cookies Policy is effective as of April 1, 2026.

I. DEFINITIONS

"**Automated Decision-Making Technology**" and "**ADMT**" means any system, software, or algorithm, including those powered by Artificial Intelligence or machine learning, that processes personal information to replace, facilitate, or execute decisions, often without direct human involvement.

"**Blockchain**" means a shared, digital ledger or record book that tracks information – such as financial transactions - across a network of computers rather than one central authority. Data is stored in "blocks" that are securely linked together in a "chain". It is immutable in that it cannot be altered and transparent, ensuring trust and security

"**Business Days**" means any day other than a Saturday or Sunday or United States federal public holiday on which banks are physically open for the transaction of general banking business. Any other day is to be considered a calendar day.

"**Crypto**" and "**Crypto Currency**" mean a digital or virtual currency secured by cryptography, operating on decentralized blockchain networks rather than relying on central authorities like banks. These, typically, peer-to-peer systems allow for secure, transparent, and immutable recording of transactions. Key examples include Bitcoin and Ethereum.

"**Fiat**" and "**Fiat Currency**" mean government-issued money not backed by a physical commodity such as gold or silver. Its value is derived from government decree (legal tender), economic policy, and public trust in the issuing authority. Examples include the U.S. Dollar, Euro, and Japanese Yen, which are used for daily transactions.

"**Shielded**" or "**Private Settlement Lay**ers" are Blockchain infrastructures that allow transactions to be processed while keeping sensitive data - such as sender, receiver, and asset amounts - encrypted and hidden from public view. Unlike public blockchains (e.g., Bitcoin, Ethereum), which reveal all transaction details, these layers use zero-knowledge ("**ZK**") proofs to verify that a transaction is valid without exposing the underlying data.

"**Stablecoin**" means a type of cryptocurrency designed to maintain a stable value by pegging it to a reserve asset, most commonly the U.S. dollar, to reduce the volatility associated with assets like Bitcoin. They act as a bridge between traditional Fiat currencies and the digital asset ecosystem, enabling faster, cheaper, and global transactions.

"**Third Party Providers**" and "**Contracted Third Party Providers**" means a commercial entity with which We have an agreement to provide certain products and services to You.

"**Thirty Day Cure Provision**" means a rule which gives businesses a Thirty (30) day window after receiving notice of a violation to fix, or "cure," the issue before facing lawsuits or penalties. It acts as a mandatory grace period to correct privacy, security, or policy deficiencies, such as unauthorized data sales.

"**Working Hours**" means 9:00 am to 5:00 pm Eastern (New York City, NY) time on Business Days.

II. GENERAL

Online privacy is constantly evolving, and Omniwire Inc., ("**Omniwire**", "**We**", "**Our**", "**Us**") a company that is organized in the state of Delaware in the United States of America, will take all commercially reasonable efforts to maintain up to date and effective online privacy standards and practices. We have linked every page of Our Website (the "**Website**") to this document for Your convenience. You may also access Our Privacy and Cookies Policy (the "**Policy**") on Our smartphone APP, Our website www.Omniwire.com and You may also contact Omniwire at legal@Omniwire.com with any questions or concerns that You may have.

Omniwire is committed to respecting Your online privacy and recognizes our customer's ("**You**" and "**Your**") need for appropriate protection and management of any personally identifiable information ("**Private Information**") that You share with Us. Private Information means any information that may be used to identify an individual, including, but not limited to; (1) a first and last name; (2) a home or other physical address; (3) an email address; (4) other contact information, whether at work or at home; (5) telephone numbers; (6) credit/debit card information; (7) bank account information; and (8) Website usernames and passwords. Omniwire collects and uses Your Private Information only for Our business purposes which allows Us to provide an eWallet, a Demand Deposit Account (e.g. a Checking Account), a Debit Card, state of the art transaction processing services and other financial services to You to enable You to make purchases of goods and services at retail merchants ("**Retailers**") and to transfer funds between authorized Omniwire accounts and to and from other financial institutions. We do not sell Your Private Sensitive Information to anyone.

If You choose to provide Us with Your Private Information through Our Website, by facsimile, mail, e-mail or any other viable method of transmission, We may transfer that Private Information within Omniwire, to Our third-party service providers, to Retailers with whom You have made transactions, or for the purpose of assisting the Retailer in resolving disputes, and from Your country or jurisdiction to other countries or jurisdictions around the world if the need arises.

We strive to comply with all applicable privacy laws around the globe that are designed to protect Your privacy. Although legal requirements may vary from country to country, We will adhere to the principles set forth in this Policy even if, in connection with the above, We transfer Your Private Information from the United States to countries that may not require as stringent levels of protection for Your Private Information as are applied Us. In other words, Our goal is to provide protection for Your Private Information no matter where that Private Information is collected, transferred, used or retained.

Omniwire may also collect government-issued identification numbers and other proofs of identity and domicile ("**ID Information**") to comply with existing Know Your Customer government and regulatory entity regulations.

Much of the material in Our Policy is similar to the General Data Protection Regulations ("**GDPR**") in the European Union regarding the safety of, use of, security of, processing of, and other specific rights regarding Your Private Information. We will, wherever possible, adhere to the guidelines and regulations set out in the European Union GDPR.

Many state privacy policies do not apply to entities where the entities' number of customers in that state are below a certain threshold or do not meet other requirements. For example, the privacy policy of the state of New Jersey does not apply if: (1) an entity does not control or process data for at least One Hundred Thousand (100,000) New Jersey consumers; or (2) control or process personal data of Twenty Five Thousand (25,000) New Jersey consumers **and** derive revenue (or receive discounts) from the sale of

personal data. However it is Our policy to implement the strictest of the data privacy laws of any state, and/or elements of the privacy laws of any state that are not included in the privacy laws of the strictest state.

Some states privacy policies allow Omniwire to follow the Thirty Day Cure Provision. However in all cases Omniwire will make all commercially reasonable attempts to cure a violation in a shorter timeframe.

Omniwire does not use any ADMT in any of Our systems that have an impact on Your Sensitive Private Information. We may use ADMT in making decisions on whether to approve or deny certain transactions You may enact while using Our Services, such as approving or denying a purchase transaction related to Our Services.

III. SPECIFIC U.S. STATE PRIVACY RULES

As of January 1, 2026 nineteen states have passed and made effective, or set dates for their policies to become effective, their own privacy and data protection laws and regulations. A summary of and Omniwire's adherence to these state laws and regulations are described below:

California: - We comply with the California Consumer Privacy Act of 2018 ("**CCPA**"), and the California Privacy Rights Act of 2020 ("**CPRA**") with its amendments to the CCPA, and its new regulations and requirements. These two acts provide California consumers with right to access, delete, and opt out of the sale of their Private Information, and businesses are required to maintain a privacy policy detailing those rights and the business's privacy practices. California's amendments took effect January 1, 2023 and were enforceable on July 1, 2023.

Colorado: - We are in compliance with Colorado's Senate bill 21-190 entitled the "**Colorado Privacy Act**" and "**CPA**" which became effective and enforceable on July 1, 2023.

Connecticut: - We are in compliance with Connecticut's Senate Bill 6 which is an Act Concerning Personal Data Privacy and Online Monitoring (also known as The Connecticut Data Privacy Act or "**CTDPA**") which went into effect and was enforceable on July 1, 2023.

Delaware: - Delaware's Personal Data Privacy Act ("**DPDPA**") was signed into law on September 11, 2023 and went into effect on January 1, 2025. We are in complete compliance with all aspects of the DPDPA.

Florida: - Florida has passed the Florida Digital Bill of Rights ("**FDBOR**") which will apply to all persons that: (i) conduct business in Florida or produce products or services used by Florida individuals or households; and (ii) process or engage in the sale of personal data. Omniwire does not sell any of Your Personal Private Data. At present Omniwire is not required to comply with the FDBOR. However, Omniwire has incorporated Florida's relevant best practices for protecting personal information into Our Privacy Policy.

Illinois: - The state of Illinois has passed the Biometric Information Privacy Act ("**BIPA**") which insures that individuals are in control of their own biometric data and prohibits companies from collecting it unless they: (i) Inform the person in writing of what data is being collected or stored; (ii) inform the person in writing of the specific purpose and length of time the for which the data will be collected, stored and used; and (iii) obtain the person's consent. Biometric information includes retina or iris scans, fingerprints, voiceprints, hand scans, facial geometry, DNA, and other unique biological information. Omniwire complies with all of the relevant requirements of BIPA.

Indiana: - Indiana has passed comprehensive legislation, the Indiana Consumer Data Protection Act ("**ICDPA**") that regulates how consumer data is collected and secured; the . Although the ICDPA went into effect January 1, 2026, it only applies to: (i) entities that control or process personal data of 100,000 or more Indiana consumers; or (ii) entities that receive Fifty Percent (50%) or more of gross revenue from selling personal data of Twenty Five Thousand (25,000) or more consumers. Omniwire meets neither of those requirements, but Omniwire is in compliance with all of the legislations' mandates.

Iowa: - We are in compliance with Iowa's Consumer Data Protection Act ("**ICDPA**") which went into effect January 1, 2025. NOTE: - Although We are not required to be in compliance with Iowa's laws at this time. We are more than compliant with Iowa's laws, as Iowa's laws are less consumer friendly that than the laws of other states with which We are in complete compliance.

Kentucky: - Kentucky passed the Kentucky Consumer Data Protection Act ("**KCDPA**") on April 4, 2024 and it went into effect January 1, 2026. The following is a link to the KCDPA for comprehensive information (https://apps.legislature.ky.gov/law/statutes/chapter.aspx?id=39092). See the section starting at .3611. Although the KCDPA went into effect January 1, 2026, it only applies to: (i) entities that control or process personal data of 100,000 or more Kentucky consumers; or (ii) entities that receive Fifty Percent (50%) or more of gross revenue from selling personal data of Twenty Five Thousand (25,000) or more consumers. Omniwire meets neither of those requirements, but Omniwire is in compliance with all of the legislations' mandates.

Maryland: - The Maryland Online Data Privacy Act ("**MODPA**") was passed May 9, 2024 and become effective on October 1, 2025 gives Maryland residents mor control over their personal data. The MODPA, like certain other State Data Privacy Laws, contains the regulatory framework of the European Union's General Data Protection Regulation. Omniwire is in compliance with all of the MODPA.

Minnesota: - The Minnesota Consumer Data Privacy Act ("**MCDPA**"), which went into effect on July 31, 2025, grants Minnesota residents significant rights over their personal data, including access, correction, deletion, and portability, and the right to opt out of targeted advertising, data sale, and certain profiling activities. The following link provides a download of a .pdf file that will provide further information: - Minnesota Consumer Data Privacy Act (MCDPA). Omniwire is in compliance with all aspects of the MCDPA.

Montana: - Montana has modeled their Privacy and Data Protection policies after Connecticut's privacy law. This act went into effect October 1, 2024 and Omniwire is in compliance with all of the legislation's mandates.

Nebraska: - On April 17, 2024, Nebraska signed into law omnibus Legislative Bill 1074, which includes the Nebraska Data Privacy Act ("**NDPA**"), making Nebraska the seventeenth state to adopt comprehensive data privacy legislation. The NDPA went into effect January 1, 2025 is similar to other state's legislation, and We are in complete compliance with all acts of the legislation.

New Hampshire: - On March 6, 2024, New Hampshire adopted a comprehensive data privacy law, when the governor signed SB 225 called the New Hampshire Privacy Act ("**NHPA**"). The law went into effect January 1, 2025, is similar to other state's legislation, and We are in complete compliance with all acts of the legislation.

New Jersey: - On January 16, 2024, New Jersey signed into law Senate Bill 332 the New Jersey Data Privacy Law ("**NJDPL**") making New Jersey the thirteenth state to adopt comprehensive data privacy

legislation. The NJDPL took effect on January 15, 2025. Although the NJDPL does not apply to Us at the time, We are in complete compliance with all aspects of the NJDPL.

Oregon: - Oregon has passed one of the strongest data privacy laws passed to date, the Oregon Consumer Privacy Act ("**OCPA**") includes provisions on biometric data, sensitive and personal data, and children's data protections, and it doesn't have the same exemptions found in other state privacy laws. The OCPA went into effect July 1, 2024 and Omniwire is in compliance with all of the legislations' mandates.

Rhode Island: - Rhode Island passed the Rhode Island Data Transparency and Privacy Protection Act ("**RIDPA**") on July 17, 2024. It will go into effect January 1,2026. Following is a link to the specifics of the law (https://webserver.rilegislature.gov/Statutes/TITLE6/6-48.1/INDEX.htm). The RIDPA is very similar to laws passed in other states including: (i) Confirmation of Processing; (ii) Access and Portability; (iii) Correction and Deletion; and (iv) the ability to Opt-Out. For more comprehensive information see the above link. The law applies to for-profit entities conducting business in Rhode Island or targeting Rhode Island consumers that either: (i) process personal information of Thirty Five Thousand (35,000) or more Rhode Island residents; or (ii) process personal information of Ten Thousand (10,000) or more Rhode Island residents while deriving more than Twenty Percent (20%) of gross revenue from the sale of personal information.

Tennessee: - Tennessee has passed comprehensive legislation that regulates how consumer data is collected and secured (the "**TIPA**"). This act went into effect July 1, 2025 and Omniwire is in compliance with all of the legislations' mandates.

Texas: - The Texas Data Privacy and Security Act ("**TDPSA**") applies to large companies that do business in Texas or sell, collect, or process personal data of Texas citizens. The TDPSA went into effect July 1, 2024 and Omniwire is in compliance with all of the legislation's mandates.

Utah: - We are in compliance with Utah's S.B. 227 – Utah Consumer Privacy Act (the "**UCPA**") which went into effect and became enforceable on December 31, 2023.

Virginia: - We comply with the Virginia Consumer Data Protection Act (Va. Code Ann. §§ 59.1-575 to 59.1-585) ("**VCDPA**") which took effect and was enforceable from January 1, 2023.

Nine state regulators are collaborating on the implementation and enforcement of their privacy laws with the shared goal of protecting consumers. The Consortium of Privacy Regulators ("**CofPR**") is a bipartisan effort that includes state Attorneys General and the California Privacy Protection Agency. Members include California, Colorado, Connecticut, Delaware, Indiana, Minnesota, New Hampshire, New Jersey, and Oregon. Omniwire is aware of the efforts of the CofPR. At this time, no relevant amendments to the involved state privacy policies have been published.

All of the above mentioned states' Privacy and Data Protection regulations are collectively referenced to in the remainder of Our Policy regarding states in the United States of America as the "**State Privacy and Data Protection Requirements**". Regulations and Our policy regarding transfer of Your Private Information outside of the country in which You reside is collectively reverenced to in the remainder of Our Policy as "**Cross Border Privacy and Data Protection Requirements**" in Section III.

The US state of California has implemented the California Invasion of Privacy Act ("**CIPA**") which prohibits eavesdropping, recording, or wiretapping of confidential communications without the consent of all parties involved. It requires all parties to a confidential communication to consent before it can be recorded or monitored, and it can be enforced through civil lawsuits and criminal penalties. The regulations regarding recording or wiretapping of confidential communications differs from US state to

state. Many states are one-party-consent-states, meaning a person can legally record a private conversation as long as they are a party to the conversation and give their consent. Under US federal law, We can legally record a private conversation as long as at least one party consents, also known as "one-party consent". This means if You are a participant in the conversation, We can record it without the Your permission.

Omniwire has implemented the key principles of the CIPA, meaning that We, and all of Our Third Party Providers, will not record any conversation with You unless You give Your permission for the conversation to be recorded. Our asking You for Your consent indicates Our implied consent to make the recording. We may ask for Your consent to record customer service queries for training and investigative purposes. Omniwire does not nor has any capability for wiretapping You.

If You refuse to provide Your consent to record a verbal communication, We, or Our Third Party Provider may choose not to provide You with verbal assistance, but require that You communicate Your query to Us, or Our Third Party Provider, via Email or other written communications.

If You live outside of the United States of America, Your country of domicile may have regulation ranging from requiring neither party's consent to regulations even more strict than the CIPA. If You have concerns about Us recording a verbal communications, please check to ascertain what are the regulations in Your country, and communicate those concerns to Us in writing via Email or government post / mail.

Wherever applicable We have implemented the requirements of the most strict of the State Privacy and Data Protection Requirements.

Several states have identified a new category of Private Information entitled "**Sensitive Private Information**" which is a subcategory of Private Information and includes but is not limited to:

- Any data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions or diagnoses, sexual activity or orientation, citizenship, or immigration status;
- Genetic or biometric data used to uniquely identify an individual;
- Personal data of a child under the age of 13;
- Information that identifies an individual's specific location with a defined degree of precision and accuracy (called "precise geolocation data").
- Social Security, driver's license, state ID, or passport numbers;
- Financial account information;
- Precise geolocation;
- Racial or ethnic origin;
- Sex life or sexual orientation;
- Religious or philosophical beliefs;
- Union membership;
- Nonpublic communication;
- Genetic, biometric, and health data (Biometric information includes retina or iris scans, fingerprints, voiceprints, hand scans, facial geometry, DNA, and other unique biological information.)

Within Our Policy, Sensitive Private Information is included collectively in the information for Private Information as is relevant. We will implement all relevant rules and regulations relating to Sensitive Private Information for Accounts of Customers and, where relevant, for any other Account no matter the domicile of the Account holder.

This Policy explains how Omniwire treats Your Private Information.

IV. STABLECOIN AND CRYPTO CURRENCIES

Our Privacy Policy regarding Stablecoins and other Crypto Currencies clearly bridge the gap between blockchain transparency and user data protection, particularly in light of new regulations such as the GENIUS Act (2025) that classify Stablecoin issuers as financial institutions under the Bank Secrecy Act ("BSA"). We are not a financial institution, as defined under the BSA, but may process Your Sensitive Private Information should You use one of Our products or services that involve Stablecoins. At this time We do not offer any products or services that involve Crypto Currencies other than Stablecoins.

Blockchain protects Your Sensitive Private Information by enabling decentralized, encrypted, and tamper-proof data management where users control their own keys. It uses cryptographic techniques like zero-knowledge proofs to verify information without revealing it, allows storing sensitive data off-chain while anchoring its integrity on-chain, and provides secure audit trails for access.

We use Blockchain technology in the management of a Stablecoin transaction. Some key aspects of how We perform this process are:

- While personal identifiers may not be on the Blockchain, wallet addresses, transaction amounts, and timestamps are public and permanent.

- If required by law and regulations, We may link Your real-world identity to Your public wallet address.

- As with traditional financial transactions, Your Sensitive Private Information is collected for Know Your Customer, Counter Terrorist Financing and Anti-Money Laundering purposes, as mandated by federal regulations.

- As with traditional financial transactions, Your Sensitive Private Information may be shared with regulatory authorities and law enforcement.

- Your Sensitive Private Information, if required by regulatory authorities and law enforcement, may be shared with Blockchain analytics companies.

- As with traditional financial transactions, We may work with our regulated financial partners to freeze or burn assets upon legal order.

- We may use Shielded or Private Settlement Layers that obfuscate transaction details while maintaining compliance with relevant regulations and laws.

V. CROSS BORDER TRANSFER OF YOUR PRIVATE INFORMATION

Your Private Information may be transferred to, and processed in, countries other than the country in which You reside. These countries may have data protection laws that are different from the laws of Your country.

By using Our services, You consent to Your Private Information being transferred to our facilities and the third parties with whom We share Your Private Information as described in this Privacy Policy.

For compliance with the General Data Protection Regulations of the European Economic Area

If You are domiciled in the European Economic Area ("**EEA**") and We transfer Your Private Information from the EEA to a country not deemed to provide an adequate level of protection by the European Commission, the transfer will be based on safeguards such as Standard Contractual Clauses ("**SCC**") approved by the European Commission or Binding Corporate Rules ("**BCRs**") implemented within Our company. You may request a copy of these clauses or rules by contacting Us using the information provided below.

Regarding law enforcement requests

Please be aware that the privacy laws in certain countries to which Your data may be transferred may not be equivalent to those in Your country. Your information may be subject to access by law enforcement and national security authorities of those jurisdictions.

If You are domiciled in the United States of America, the U.S. Department of Justice recently implemented new rules under Executive Order 14117, aiming to control how sensitive personal data gets transferred outside the U.S. - especially when it ends up in the hands of people or entities in countries such as China, Russia, Iran, North Korea, Cuba, and Venezuela (hereinafter "**Countries of Concern**". It's a direct response to national security risks tied to mass data access. The rule targets transfers involving bulk sensitive information, including but not limited to biometric data, health records**,** financial details, and even precise location on Your location. If We encounter a situation where it is possible that Your Private Information might be transferred to Countries of Concern, We will inform You in advance of this possible transfer situation. You may opt out of allowing this transfer to happen by contacting US at legal@Omniwire.com.

VI. PRINCIPLES

Omniwire's General Privacy Principles:

Omniwire is committed to safeguarding the privacy of Your Private Information:

- We will only collect and use Your Private Information where We have lawful grounds and legitimate business reasons to do so;
- We will be transparent in Our dealings with You and will tell You about how We collect and use Your Private Information;
- If We have collected Your Private Information for a particular purpose, We will not use it for any other purpose unless You have been informed and, when required by law, Your permission has been obtained;
- We will not ask for more Private Information than We need for the purposes for which We are collecting it;
- We will update Our records when You inform Us that Your details have changed;
- We will continue to review and assess the quality of Your Private Information;
- We will implement and adhere to information retention policies relating to Your Private Information and will ensure that Your Private Information is securely disposed of at the end of the appropriate retention period;
- We will observe the rights granted to You under applicable privacy and data protection laws and will ensure that We promptly and transparently deal with queries relating to privacy issues;

- We will delete Your Private Information when You request Us to do so, with the exception of when We are required by law to retain some or all of Your Private Information for certain periods of time;
- We will train Our staff on their privacy obligations;
- We will ensure We have appropriate physical and technological security measures to protect Your Private Information regardless of how it is processed or where it is stored;
- We will ensure that when We outsource any processes, the supplier has appropriate security measures in place and will contractually require them to comply with Our privacy principles;
- We will ensure that suitable safeguards are in place before any of Your Private Information is transferred to any other entity or to any other countries;
- We will provide Account holders from California with a link on Our Website entitled "Limit the Use of My Sensitive Private Information" which will explain their modified and/or expanded rights;
- We have implement cybersecurity safeguards;
- We have created and communicated to consumers a process by which consumers may submit a request regarding their Private Information and subsequently appeal any decision made by Us;
- We provide a clear and conspicuous notice informing consumers that they have the right to opt out of targeted advertising and sales of their personal data;
- We have a user-selected universal opt-out mechanism;
- We update Our Privacy Policy to explain Our collection and use of Your Personal Information;
- We update Our contracts with third parties to ensure that these third parties comply with all relevant data privacy laws; and
- We have established a procedure to determine when to conduct a data protection assessment.

To protect Your privacy, We have adopted the following core areas of focus:

1. Notice
2. Choice
3. Security
4. Access and Accuracy

1. Notice

<u>Information Collection</u>

You may access and browse certain parts of Our Website without disclosing any Private Information. However, if You sign up for an Omniwire Account, We will require that You supply Us with some Private Information. You will be required to input at a minimum: (1) Your full legal name; (2) the address where You currently reside which includes Your street address, apartment number if applicable, Your City, State and Zip Code; (3) Your telephone number; (4) Your date of birth, and (5) a color picture of a current government issued identity document, and other information at Our discretion.

If You attempt to purchase a product or service offered by a Retailer, We may request that You voluntarily supply Us or one of Our service providers with other Private Information, specifically Your method of payment details. We use a secure transmission method for all of Our transmissions. You will be required

to allow Us to store Your payment mechanism information (for example, credit card number and expiration date) so that You are not required to reenter this information on a subsequent purchase transaction. If You opt not to allow Us to store this information You will be required to reenter Your payment details during each merchandise process.

We receive and store all information that You enter in Our Website unless You specifically opt-out of providing Us Your payment method details. In addition, We collect information about You during Your visit, such as Your IP Address, and We employ special purpose software in order to ascertain Your physical location when using Our Website. Also, We may collect nonpublic Private information about You from the following sources:

- Information We receive from You on applications or other forms; and
- Information about Your transactions with Our third party suppliers, Retailers, or others.

In the process of accepting You as a Customer, We and/or Our third party suppliers may collect information about You from sources such as social media and public records. You are required to provide US and Our third party suppliers with accurate and up-to-date information, and Your failure to accurately provide such information could result in the voiding of Your agreement with Us and the cancellation of Your Account.

We will require You to provide required Private Information through Our Website or on Our APP. Only in situations where You cannot scan and upload this Private Information online to Us, will We request or accept Private Information by any other methods such as E-Mail, physical mail or via facsimile message. Private Information collected via facsimile, mail, or e-mail will be scanned and stored in Our computerized databases, and any paper copies will be shredded unless We are required by law to keep paper copies.

Current government regulations require Us to collect valid government-issued identification document / numbers ("**ID Numbers**") such as passport numbers, driver's license numbers and/or other government issued forms of identification of its Account holders as a preventative measure against identity theft, money laundering, terrorist financing, and the use of Our products and services for illegal purposes. WE WILL NEVER ASK YOU FOR YOUR ID NUMBER OVER INSTANT MESSENGER OR E-MAIL. You may be prompted to enter Your ID Number after You log into Your Omniwire Account, or upon sign-up for a new Omniwire account.

Information Use

Omniwire is the sole owner of the information collected through Our Website, Our smartphone APP, or any other means. We will not sell, share, or rent this information to third parties, except as set forth in this Policy. We will release data when required by law, to enforce Our agreement(s) with You, or to enforce the contract rights of Our Retailers or third party suppliers.

Information Sharing

Omniwire will not share Your ID Number or government-issued identity document with anyone, other than a government institution or authority when required by law, through subpoena by a court of competent jurisdiction, or other regulation.

We ensure that Your Private Information will not be disclosed to anyone other than a government institution or authority when required by law or other regulation, except We may disclose Your Private Information to the following parties ("**Third Parties**"):

- Our affiliated bank and payment system processors as required to process transactions on Your payment method with Our Retailers;
- Retailers affiliated with Us from which You are purchasing goods and services using Our services.

In addition, We may disclose Your user name, name, address, phone number, and E-Mail address to non-financial companies, such as companies that perform marketing services on Our behalf ("**Nonaffiliated Third Parties**") to provide You information, special offers, and promotions. You may opt-out from these disclosures at any time by following the procedures detailed in the Access, Verification, Timing and Costs, Opt-Out Procedures section of this Policy.

2. Choice

Choice to provide Private Information

You may choose whether or not to provide Your Private Information to Us. If You choose not to provide the Private Information We request, You can still visit portions of Our Website, but You may be unable to access certain options, offers, and services that involve Our interaction with You. If You chose to have a relationship with Us, You will be required to provide certain Private Information in connection with such relationship in order to maintain that relationship.

In those situations where governmental regulations require You to provide ID Information, if You choose not to provide this ID Information, You will cannot be provided an account. If You are a current Omniwire account holder, and We request Your ID Information upon login, if You choose not to provide the requested ID Information within the time allocated, We will terminate Your Omniwire Account and You will not be able to use Your Account.

Use of Your Information:

If You prefer that We not disclose non-public Private Information about You to Nonaffiliated Third Parties, You may opt out of those disclosures; that is, You may direct Us not to make those disclosures (other than disclosures permitted or required by law). If You wish to opt out of disclosures to Nonaffiliated Third Parties, You may opt-out by contacting Us by following the procedures detailed in the Access, Verification, Timing and Costs, Opt-Out Procedures section of this Policy.

3. Security

Omniwire has implemented best-practices security policies, rules and technical measures to protect the Private Information that We have under Our control from unauthorized access; improper use or disclosure; unauthorized modification; unlawful destruction or accidental loss. Secure Socket Layer (SSL) software is used when receiving and transmitting electronic payments. The sensitive information that You provide is encrypted.

Access to Your Private Information is highly restricted. Our facilities are only accessible through a process of security clearance. All employees and data processors, who have access to and are associated with the processing of Private Information are obliged to respect the confidentiality of Our customers' Private Information and Your Private Information and ID Information is restricted to those employees who have a need to know Your Private Information. We conduct background and credit checks on all of Our employees prior to employment. We employ a User ID, password scheme and a random Token

process in order to limit and achieve access to Our computer networks by Our employees and Third Parties.

PCI-DSS Compliance

The Company is and has been in compliance with all applicable portions of the Payment Card Industry Data Security Standard ("**PCI-DSS**") in all material respects, as it has been amended from time-to-time. With respect to payment card transactions or information processed in any way (including any processing, storing or communication of transaction data or Cardholder Data (as such term is defined in the PCI-DSS)), by Us, We are in material compliance with the PCI-DSS applicable to service providers and with the requirements related to PCI-DSS in each Agreement pursuant to which We provide services of any kind. Each of Our products or services that is:

- intended to be used to process financial or payment card transactions (including any processing, storing or communication of transaction data or Cardholder Data (as such term is defined in the PCI-DSS)); and
- provided by the Company to any person or business, is in compliance with the PCI-DSS.

SOC-2 Type 1 Compliance

"SOC 2" stands for System and Organization Controls 2. It was created by the American Institute of Certified Public Accountants ("**AICPA**") as a way to help organization's verify their security and reduce the risk of a security breach.

SOC 2 Type 1 compliance evaluates an organization's cybersecurity controls at a single point in time. *The goal was to determine whether the internal controls that We have put in place to safeguard customer data are sufficient and designed correctly*.

We completed our SOC 2 Type 1 audit in 2024 and are now SOC 2 Type 1 compliant in all respects. We are currently undergoing preparations for Our SOC 2 Type 2 audit.

4. Accuracy and Access

Accuracy

The Private Information, that You provide Us must be accurate and current. Our goal is to provide You a means of access should You need to update or correct Your Private Information. If for any reason those means are unavailable or inaccessible, You may send updates and corrections about Your Private Information to legal@Omniwire.com or by facsimile, by governmental or private express mail, and all reasonable efforts will be made to incorporate the changes in Your Private Information as soon as practicable.

Access, Verification, Timing and Costs, Opt-Out Procedures

How to Submit a Request Regarding Your Private Information. To submit an access or deletion request, please email legal@Omniwire.com. To submit a "Shine the Light" request, email Us at legal@Omniwire.com. If You designate an authorized agent to make an access or deletion request on Your behalf using one of the channels described above, We will require You to provide the authorized agent written permission to do so and to verify Your own identity directly with Us (as described below). For questions or concerns about Our privacy policies and practices, please contact Us as described in the 'How to Contact Us' section of Our Policy.

Verifying Requests. To help protect Your privacy and maintain security, We will take steps to verify Your identity before granting You access to Your personal information or complying with Your request. We will require You to provide any of the following information: Your name, date of birth, the last four digits of Your Social Security number, the email and physical addresses associated with Your Omniwire Account, one or more recent transactions, and the last four digits of one or more Omniwire-branded cards associated with Your Account. If You have never had an account with Us and You request access to or deletion of Your personal information, there is no reasonable method by which We can verify Your identity to the level of certainty required by the relevant regulations. The reason for this is that Omniwire does not maintain information about non-accountholders in a way that is linked to named actual persons (and historically has not linked IP addresses, device identifiers or other information collected by automated means to named actual persons). In addition, if You ask Us to provide You with specific pieces of personal information, We may require You to sign a declaration under penalty of perjury that You are the consumer whose personal information is the subject of the request.

Timing and Costs. Within five (5) business days of Our receipt of Your request, You shall be provided a copy of the Private Information and/or ID Information that is kept about You. If You agree to receive this information in electronic format, You will not be charged. However, if You require that the information is sent to You in paper format, You will be charged a $25 processing fee to complete the request. Except for when required by relevant law regarding Your Private Information, Omniwire reserves the right to refuse any request for information, and We will communicate the reason for Our decision to You.

Opt-Out Procedures. If You desire to opt out of or modify any uses of Your Personal information contact Us via Email at legal@Omniwire.com and explain, in detail, Your request.

VII. YOUR RIGHTS

You have the right to:

- Access Your Private information. You have the right to obtain from Us confirmation as to whether or not Your Private data is being obtained, stored, processed and retained, and, where that is the case, access to the Private data.
- Correct and/or complete Your Private information. You have the right to correct any of Your Private information that You believe to be inaccurate. This includes the right to have incomplete Private information completed.
- Opt Out. You have the right if You live in certain states to completely opt out not only of the sale of Your Personal Information but also of the collection and use of Your Personal Information. Be advised that if You completely opt out of Our being able to collect and use Your Personal Information, You may not be able to utilize some of our services.
- Require Us to restrict how We use Your information. You have the right to restrict the processing or use of Your Private information where one of the following applies. You believe that:
    - the accuracy of Your Private information is contested by You, for a period enabling the Company to verify the accuracy of Your Private information;
    - the processing is unlawful and You oppose the erasure of Your Private information and request Us to restrict its use instead;
    - We no longer need Your Private information for the purposes that Were disclosed to You in this Policy, unless certain of Your Private information is required by Us for the establishment, exercise or defense of legal claims;

- Obtain copies of Your Private information that We have. You can ask Us for a copy of Your Private information and We will provide that information in machine readable form. See the above section 4 – Access regarding any costs associated with this request.
- Right to delete some of Your Private information. You can ask Us to erase or delete all or some of Your Private information where one of the following applies. Some of Your Private information may not be able to be deleted for Us to comply with relevant law and processing regulations.
    - Your Private information is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    - There is no legal ground for the Us to use, retain or process Your information;
    - Your Private must be erased for compliance with a legal obligation in law to which the We are subject;
- Right to Access Information About Automatic Decision Making. You now have the right to access information about how companies use automated decision-making technology. You have the right to opt-out of any automated decision-making processes.
- Right to Data Portability. You now have the right to request that We transfer Your Private personal to another entity, to the extent it is technically feasible.
- Right to lodge a complaint. You have a right to lodge a complaint with the supervisory authority of the state in which You reside.
- Right of non-discrimination. You have the right of non-discrimination by Us for exercising Your Privacy information management rights.

VIII. THIRD PARTIES

Occasionally, We receive information from Third Parties to compare to Your Private Information that You have provided to Us for fraud prevention purposes.

Any Websites displayed to You by Our Website as Internet search results or linked to Internet search results pages provided to You by Our Website, including Websites owned or operated by Our clients, or Websites developed by Third Parties over which We exercises no control. Such Websites may send their own Cookies to end-users, collect data, or solicit Private information from You (see Our Cookies Policy for information on Our use of Cookies). We is not responsible for the privacy practices or the content of such Websites, including such Websites' use of any information collected when You are directed to or click through to such Websites. Our inclusion of such links does not imply endorsement. Even though such information might not identify You personally, You are strongly encouraged to become familiar with the privacy practices of those Websites.

IX. CHILDREN

Omniwire, in compliance with the US federal law, the Children's Online Privacy Protection Act ("**COPPA**"), does not request, or knowingly collect Private Information from children under the age of thirteen (13) years. We take specific steps to protect the privacy of children by making reasonable efforts to ensure that a child's parent or legal guardian has authorized the collection and/or distribution to Third Parties of a child's Private Information. Additionally, to ensure that children's privacy is respected on Our Website, We require age verification on every inquiry. Furthermore, We do not give children the ability to post messages or otherwise distribute information about themselves on Our Website.

X. POLICY CHANGES

Omniwire will make all commercially reasonable efforts to maintain up-to-date and effective privacy standards and policies. Whenever We makes changes to these standards or this Policy We will post a notice of this change at www.Omniwire.com. For the time You have an account with Us, You are agreeing to this Policy and changes that may be made to this Policy.

XI. EFFECTIVE DATES

This Policy is effective immediately. Policy changes are effective as soon as they are posted on Our Website unless a specific effective date is provided.

XII. COMMITMENT

Omniwire is committed to the privacy of all customers' Private Information and are actively supporting current industry initiatives to preserve individual privacy rights on the Internet. Protecting Your privacy online is an evolving area, and Our Website is constantly evolving to meet these demands.

If You have any comments or questions regarding this Policy, please contact legal@Omniwire.com. While We cannot guarantee privacy perfection, We will address any issue to the best of Our abilities as soon as possible.

XIII. ARTIFICIAL INTELLIGENCE POLICY

Omniwire uses artificial intelligence ("**AI**") systems such as Our proprietary developments in AI to provide You enhanced experiences in Your interactions with Our Customer Service system and Your use of Our APP.

Compliance with state and federal AI use policies.

At this time there are no regulations at the Federal level and few at the state level. AI legislation generally aims to address concerns related to safety and security, responsible innovation, and preventing algorithmic discrimination.

Omniwire is in the process of developing a comprehensive Artificial Intelligence Privacy and Usage policy which will be published on Our website and on the APP on or before 1 July 2025.

XIV. COOKIES

"**Cookie**" means a small piece of text data stored on the storage drive of a visitor to a Website, containing information about the visitor that can only be read by the server that placed the information onto the visitor's storage drive. We employ Cookie technology.

Most browsers are initially set up to accept Cookies. You can set Your browser to block Cookies entirely, delete Cookies when You leave the Website, notify You when You receive a Cookie giving You the chance to decide whether or not to accept it, or limit the subsequent retrieval of Cookies by the Website. In addition, there are number of privacy-enhancing tools and software that You may purchase that will enable You to identify and block Cookies on a selective basis. Please note that for some Websites that require an authorization, Cookies are not optional. Users choosing not to accept Cookies will probably not be able to access those Websites where Cookies are not optional.

Cookies can be "**Persistent**", "**Session**" or "**Essential"** Cookies.

Persistent Cookies, also called a Permanent Cookie, or a Stored Cookie, is a Cookie that is stored on Your hard drive until it expires (persistent cookies are set with expiration dates, but that date may be far in the future) or until You delete the Cookie.

Session Cookies are also called a Transient Cookie, and is a Cookie that is erased when You close Your Web browser. A Session Cookie is stored in temporary memory and is not retained after Your browser is closed. Session Cookies do not collect information from Your computer.

Essential Cookies are Persistent or Session Cookies that We may use to authenticate You and prevent fraudulent use of Your account.

To avoid any future Persistent Cookies being placed onto Your hard drive from Our Website, You may "**Opt Out**." In order for You to receive the Opt Out Cookie You will need to have JavaScript and Cookies enabled in Your browser. By receiving this Cookie, Our systems will know that You have opted out and will not attempt to assign other Cookies in the future. Since the Opt-Out Cookie does not contain a unique User ID number, it does not allow Us to identify Your computer individually. Please note again that some of Our Websites require use of Cookies, and use of Cookies is not optional (for example, a shopping cart). Account holders opting out of future Cookies will probably not be able to access those Websites.

IX.1 How Omniwire uses Cookies

When You use and access the Service, We may place a number of Cookies in Your Web browser.

We use Cookies for the following purposes: (1) to enable certain functions of the service; (2) to provide analytics; (3) to store Your preferences; and (4) to enable advertisements delivery, including behavioral advertising.

We use both Session and Persistent Cookies on the service and We use different types of Cookies to run the service:

IX.2 Third-party Cookies

In addition to Our own Cookies, We may also use various third-party' Cookies to report usage statistics of the Service, deliver advertisements on and through the service, and so on.

IX.3 What are Your choices regarding Cookies

If You'd like to delete Cookies or instruct Your Web browser to delete or refuse Cookies, please visit the help pages of Your Web browser.

Please note, however, that if You delete Cookies or refuse to accept them, You might not be able to use all of the features We offer. You may not be able to store Your preferences, and some of Our Webpages might not display properly.

IX.4 Where can You find more information about Cookies?

You can learn more about Cookies from the following third-party Websites:

- All About Cookies: http://www.allaboutCookies.org/

- Network Advertising Initiative: http://www.networkadvertising.org/

XV. How to Contact Omniwire

You can contact Us by the following methods:

Email: - legal@Omniwire.com
US Mail: - 10 Crawfords Corner Rd, P.O. Box 243, Holmdel, NJ 07733