MOTOVERSE

Motoverse USA Corp.

# Privacy Policy

9-19-23

(For Internal Use Only)

# Table of Contents

## Version Control History

| Version | Policy Number | Owner | Scope of Review/Changes | Approver | Effective Date |
|---|---|---|---|---|---|
| | | | | | |

# 1. Purpose

This Privacy Policy ("Policy") outlines the compliance requirements associated with [Insert Fintech Name]'s product offering to customers. [Insert Fintech Name] ("Company") partners with Solid Financial Technologies, Inc. ("Solid") as a BaaS provider and bank partners to enable them to offer financial products and services to their end customers.

The Policy sets out how the Company will comply with privacy laws and regulations, such as Gramm-Leach Bliley Act and its implementing regulation, Regulation P, and the FTC Safeguards Rule, the Right to Financial Privacy Act ("RFPA"), and other privacy and other applicable federal and state consumer financial privacy statutes, laws, and regulations (collectively, the Regulations) associated with its product offering.

The Policy covers how and when the Company will collect, retain, process, share, protect and transfer customers' personal data, including nonpublic personal information (NPPI). The Policy is to be used internally by Company and its employees but also requires Company to separately maintain a publicly available external Privacy Policy Statement on Company's website, as well as a consumer privacy notice to be shared directly with consumers, as applicable.

# 2. Scope

This Policy governs the Company business activities and applies to all Company employees, regardless of tenure, position, or employment status and applies to all Company's products and services. When the Company engages an affiliated or non-affiliated vendor or third-party service provider to perform services on behalf of Company, Company is responsible for ensuring that the Servicers have adequate and effective controls in place to substantially meet the requirements of this Policy.

# 3. Solid's Program Management Oversight

Company agrees to adhere to Solid's policies, procedures, and requirements as detailed in the Master Services Agreement (MSA) and onboarding documentation, including all program management requirements.

Solid is required to comply with its bank partner(s) requirements which may be subject to change. As such, the contents of this Policy may change and Company is responsible for staying updated and adapting to these changes in a reasonable timeframe, as notified by Solid.

This document does not supersede the MSA or any other agreement between the Company and Solid. The Company should refer to these agreements for a complete understanding of its responsibilities.

# 4. Fintech Procedures

| **Fintech Procedures for Privacy** |
| --- |
| **Consumer Products** |

| **Fintech Procedures for Privacy** |
| --- |
| 1. Provide consumer Privacy notices (Reg P Model Form) at such time that the customer relationship is entered.<br>   a. Provide Opt-Out Notice, as applicable, based on information sharing and the ability for the consumer to limit sharing.<br>2. Ensure consumer privacy notice is publicly available on Company's website.<br>3. Provide an Annual Privacy Notice to customers that accurately reflects Company's privacy policies and practices during the continuation of the customer relationship, unless the Company's privacy practices have not changed since the last customer disclosure.<br>4. If It is Company's policy to market products or services to children under 13 in accordance with COPPA requirements, Company will follow the requirements as noted below in this Policy.<br>5. If Company is covered under the California Consumer Privacy Act (CCPA/CPRA), Company shall comply with the provisions of the Acts which, in part, require notices explaining privacy practices in conjunction with the requirements.<br><br>**Commercial Products**<br><br>1. Provide Company's Privacy notices at account opening or with terms and conditions.<br>2. Ensure Company privacy notice is publicly available on Company's website. |

# 5. Key Terms

- **Consumer** - An individual who seeks to obtain a financial product or service from Company and has provided Nonpublic Personal Information (NPPI) to Company in seeking to obtain an account or other access to Company's products and services.
- **Customer** - A consumer who has a continuing relationship with Company that involves Company providing one or more financial products.
- **Nonpublic Personal Information ("NPPI")** - Any information that a consumer provides to Company to obtain a financial product or service from Company; information about a customer resulting from a transaction involving Company and the customer; and other information obtained about a customer in connection with Company providing financial products and services to the customer.
- **Personal data** - Any data or information considered to be personal in nature and not subject to public availability. Personal information includes, but is not limited to
    - Individual names
    - Social Security numbers
    - Credit or debit card numbers
    - State identification card numbers
    - Driver's license numbers
    - Dates of birth
    - Income

# 6. Gramm-Leach-Bliley Act

Title V of Gramm-Leach-Bliley Act ("GLBA") generally prohibits any financial institution, directly or through its affiliates, from sharing non-public personal information about its customers with a non-affiliated third party. Company values its customers and is committed to protecting the privacy of personal information in compliance with GLBA. Company is committed to ensuring the continued protection and safeguarding of our customers' NPPI.

The GLBA also implements the FTC's Safeguards Rule that requires companies to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. See Company's Information Security Policy for more information on its data security controls.

**Privacy Notices**
Subject to certain exceptions, Company is required to provide the following disclosures to customers, as defined in the Regulation, at such time that the customer relationship is entered or before a customer's information is shared with any non-affiliated third party:

- Initial Privacy Notice
    - How Company obtains and gathers information.
    - The circumstances under which Company may share information; and
    - Instructions on how to limit the information sharing.
- Opt-Out Notice
    - Initial Notice: at the time, initial disclosures are provided.
    - Annual Notice: at least annually, until the relationship is terminated; and
    - Change in Policy Notice: within 30 days of a material change in Company's policy regarding information collection, use or disclosure.

Additionally, the Regulation requires that Company provide an Annual Privacy Notice to customers that accurately reflects Company's privacy policies and practices not less than annually during the continuation of the customer relationship, unless the Company's privacy practices have not changed since the last customer disclosure.

Company will implement procedures to provide the applicable disclosures in a manner consistent with the regulation, and to record a customer or consumer's election to opt out of information sharing.

**Limits on Disclosures**
Subject to exceptions provided in the Regulation, Company may not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third-party unless:

1. Company has provided to the consumer an initial privacy notice;
2. Company has provided to the consumer an opt-out notice;
3. Company has given the consumer a reasonable opportunity before it discloses the information to the nonaffiliated third-party to opt-out of the disclosure; and
4. The consumer does not opt-out.

# 7. Right to Financial Privacy Act

The Right to Financial Privacy Act (12 USC 3401, 12 CFR 219, 29 CFR 19, 31 CFR 14)

establishes specific procedures for federal government authorities to follow when seeking member records. Company will ensure that it has procedures implemented to adequately respond to a federal agency's request for a customer's financial information.

To gain access to a member's records, the RFPA requires, with certain exceptions, that the federal government agency obtain one of the following:

- An authorization signed and dated by the member, which identifies the records being sought, the reasons the records are being requested, and the member's rights under the Right to Financial Privacy Act (The agency's request should be on an official form and contain the required member authorization.);
- An administrative subpoena or summons;
- A search warrant;
- A judicial subpoena;
- A formal written request by a government agency (to be used only if no administrative summons or subpoena authority is available).

Notwithstanding any of the exemptions provided in the RFPA, if Company receives a request for information from a federal agency, it may not release the financial records of a member until the federal government authority seeking the records certifies in writing that it has complied with the applicable provision of the Right to Financial Privacy Act.

# 8. Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act (COPPA) applies to operators of commercial websites and online services (including mobile apps and IoT devices) directed to children under 13 that collect, use, or disclose personal information from children. It is Company's policy to ensure that it markets products or services to children under 13 in accordance with COPPA requirements. Company will maintain the following for its products or services that are offered to children under 13:

- Maintain a website privacy policy that aligns with COPPA requirements.
- Maintain a website privacy policy that provides notice of what data is collected, how it is used, and when and how it is disclosed to others.
- Provide parents with a direct notice of information practices prior to collecting any information on a child under 13.
- Obtain verifiable consent from a parent prior to collecting data from children.
- Provide parents with a way to review the information collected from their children, and to demand that it be deleted.
- Provide parents with an opportunity to prevent further use or online collection of a child's personal information;
- Establish procedures to protect the security and privacy of data collected from children.
- Securely dispose of personal information of children under 13 once the information is no longer needed for a legitimate purpose.
- Not condition a child's participation in an online activity on the child providing more information than is reasonably necessary to participate in that activity.

# 9. California Consumer Privacy Act

In addition to Regulation P as stated in this policy, Company shall comply with the provisions of California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA). Company shall provide to California residents notices explaining privacy practices in conjunction with the requirements of CCPA/CPRA along with Company's obligations as described in this policy under

Regulation P in an integrated privacy policy. Company shall disclose to California residents, as applicable:

- The right to know about the personal information a business collects about them and how it is used and shared.
- The right to delete personal information collected from them (with some exceptions).
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA/CPRA rights.

# 10. Relation to Other Laws

## 10.1. Fair Credit Reporting Act and FACTA

The Fair and Accurate Credit Transaction Act ("FACTA"), which amends the Fair Credit Reporting Act (FCRA), establishes numerous requirements that provide protection for the victims of identity theft, provide more information to customers about credit reports and credit scoring, limits sharing of information with affiliates, and protects customer medical and other information. See Company's Marketing Policy which outlines FCRA in further detail and for additional details on affiliate sharing.

## 10.2. USA Patriot Act

To help the United States government prevent fraud and fight the funding of terrorism, money laundering and related activities, Section 326 of the U.S.A. Patriot Act requires that Company obtain, verify, and record information that identifies each person or entity that applies for a product through Company. Company will obtain the required information for both consumer and commercial customers as required by the USA Patriot Act. If the customer fails or refuses to provide such information, Company may decline to open an account or continue a customer relationship with said customer. See Company BSA/AML Policy for additional details.

# 11. Training

Training employees to adhere to the requirements of this policy is a crucial element in building a strong Compliance Program and a lasting culture of compliance. Company requires all employees, affiliates, and service providers to receive training as is appropriate for their roles and/or responsibilities. Reporting of completion of training is required to be made to Solid and/or its bank partners, as appropriate. For more information on training schedules and requirements, see the Compliance Training Policy.

# 12. Record Retention

Company will maintain documents accessible to all persons who are legally entitled to access them for the period required by law, or as required by Solid's Document Retention Policy, whichever is longer, in a form capable of being accurately reproduced for later reference.

# 13. Exceptions

Generally, there are no exceptions to this policy. However, in certain circumstances, Solid's Head of Compliance (or designee) may reasonably determine that a Policy exception is warranted based on specific request from Company. If an exception is granted, Company will keep a log of any exceptions approved.

Notwithstanding the foregoing, under no circumstances does Company allow Policy exceptions that would result in a violation of law.

Any questions related to this policy must be directed to Solid's Compliance team.

**Motoverse Consumer Privacy Notice**

Rev. November 2022

# FACTS

## WHAT DOES Motoverse DO WITH YOUR INFORMATION?

| | |
|---|---|
| **Why?** | Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do. |
| **What?** | The types of personal information we collect and share depend on the product or service you have with us. This information can include:<br>• Social Security number and income<br>• Account balances and payment history<br>• Credit history and credit scores |
| **How?** | All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Motoverse chooses to share; and whether you can limit this sharing. |

| Reasons we can share your personal information | Does Motoverse share? | Can you limit this sharing? |
|---|---|---|
| **For our everyday business purposes—** such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus | Yes | No |
| **For our marketing purposes—** to offer our products and services to you | Yes | No |
| **For joint marketing with other financial companies** | Yes | No |
| **For our affiliates' everyday business purposes—** information about your transactions and experiences | No | We Don't Share |
| **For our affiliates' everyday business purposes—** information about your creditworthiness | No | We Don't Share |

| | | |
|---|---|---|
| **For our affiliates to market to you** | No | We Don't Share |
| **For nonaffiliates to market to you —** information about your transactions and experiences | Yes | Yes |

| | |
|---|---|
| **To limit our sharing** | **Visit us online: https://motoverse.us/privacy.pdf**<br><br>Please note:<br>If you are a *new* customer, we can begin sharing your information 30 days from the date we sent this notice. When you are *no longer* our customer, we will continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing. |
| **Questions?** | **Go to: https://motoverse.pro** |

| | |
|---|---|
| **Who we are** | |
| **Who is providing this notice?** | **Motoverse** |
| **What we do** | |
| **How does Motoverse protect my personal information?** | To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. |
| **How does Motoverse collect my personal information?** | We collect your personal information, for example, when you<br>• Open an account or give us your income information<br>• Provide account information or pay your bills<br>• Use your credit card<br><br>We also collect your personal information from others, such as credit bureaus, affiliates, or other companies. |
| **Why can't I limit all sharing?** | Federal law gives you the right to limit only:<br>• Sharing for affiliates' everyday business purposes—information about your creditworthiness<br>• Affiliates from using your information to market to you<br>• Sharing for nonaffiliates to market to you<br>State laws and individual companies may give you additional rights to limit sharing. See below for more on your rights under state law. |

| | |
|---|---|
| **What happens when I limit sharing for an account I hold jointly with someone else?** | Your choices will apply to everyone on your account. |
| **Definitions** | |
| **Affiliates** | Companies related by common ownership or control. They can be financial and nonfinancial companies.<br>• **Motoverse** has no affiliates. |
| **Nonaffiliates** | Companies not related by common ownership or control. They can be financial and nonfinancial companies.<br>• Non affiliates we share with can include our financial banking partners or retail partners |
| **Joint marketing** | A formal agreement between nonaffiliated financial companies that together market financial products or services to you.<br>• Our joint marketing partners include our banking partners. |
| **Other important information** | |
| **For California Customers.** If your account has a California mailing address, we will not share personal information we collect about you except to the extent permitted under California law.<br><br>**For Vermont Customers**. We will not disclose your personal information or financial information to nonaffiliated third parties to market to you, other than as permitted by Vermont law, unless you authorize us to make those disclosures. | |