EU-U.S. DATA PRIVACY FRAMEWORK POLICY

SECTION I - INTRODUCTION

AscendantFX Capital USA, Inc. (Ascendant) complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) as set forth by the U.S. Department of Commerce. Ascendant has certified to the Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) regarding the processing of personal information received from the European Union in reliance on the EU-U.S. DPF. If there is any conflict between the terms in this policy and the EU-U.S. DPF Principles, the EU-U.S. DPF Principles shall govern. To learn more about the EU-U.S. DPF program, and to view our certification, please visit www.dataprivacyframework.gov.

SECTION II – OUR COMPANY

Ascendant offers foreign exchange and international payment solutions that combines tailor-made technology, dedicated customer support and seamless accounting integration to deliver speed, comprehensive reporting and clear ROI.

SECTION III – OUR COMMITMENT TO PRIVACY

I. NOTICE - We publish online (www.ascendant.world) privacy notices containing specific information about our participation in the EU-U.S. DPF, our practices around collecting, using, and sharing your personal information with third parties, our privacy practices, including an individual's rights to access and correct information, and the choices we make available to individuals regarding limiting information collection and use.

II. CHOICE – We provide individuals with a mechanism to opt out of having personal information disclosed to a third party or used for a materially different purpose than that for which it was provided. We obtain an individual's opt-in consent with respect to the sharing of sensitive information, including with a third party or its use for a new purpose. **Requests to access, correct, amend, delete, or limit the use and disclosure of personal information may be submitted to privacy@ascendant.world.**

III. ACCOUNTABILITY FOR ONWARD TRANSFER – Ascendant is responsible for the processing of personal information it receives, under the EU-U.S. DPF, and subsequent transfers to third parties acting as agents on Ascendant's behalf. Ascendant complies with the EU-U.S. DPF Principles for all onward transfers of personal information from the EU, including the onward transfer liability provisions. In certain situations, Ascendant may be required to disclose personal information in response to lawful requests by public authorities, including to meet

national security or law enforcement requirements (refer to "Disclosure to Third Parties" in Section IV.3 for more details).

IV. SECURITY – We will take appropriate physical, technical, and organizational measures to protect your personal information from loss, misuse, unauthorized access or disclosure, alteration, and destruction.

V. DATA INTEGRITY AND PURPOSE LIMITATION – We will take reasonable steps to limit processing to the purposes for which it was collected and ensure that personal data is reliable for its intended use, and that it is accurate, complete, and current. We will only retain personal information for as long as needed for the purpose of collection and as required by law and adhere to the EU-U.S. DPF Principles for as long as we retain such information.

VI. ACCESS – We will provide ways for you to access your personal information by law to enable you to correct, amend, or delete information that is either inaccurate or processed in violation of the EU-U.S. DPF Principles.

VII. RECOURSE, ENFORCEMENT AND LIABILITY – See section IV.6 below.

To learn more about our privacy practices, see our Privacy Policy details at: www.ascendant.world/compliance#privacy.

SECTION IV – COLLECTION AND USE OF PERSONAL INFORMATION

IV.1 Why We Collect Personal Information

Ascendant collects your personal information as necessary to provide you with excellent service. Ascendant will notify you at or before the time of collection of the purposes for which personal information is collected. We may collect personal information, for example:

- To establish a personal relationship with you and verify your identity
- To efficiently deliver the services you have requested
- To meet regulatory requirements
- To develop and manage products and services to meet your needs
- To contact you about products and services that might be of interest
- To grant credit where it has been requested

IV.2 What Information We Collect and How We Use It

Ascendant may collect personal information directly from you, from other financial institutions, from government agencies, from products and services that you use or request, from credit bureaus or from references that you have provided to us.

The types of personal information we collect and share depend on the product or service you have with us and the requirements of law. This may include the following information collected from you and from your transactions with us:

- Your name, mailing address, city, country, postal code, email address, and phone number
- Social Security Number (SSN) and/or Tax Identification Number (TIN)
- Driver's license and/or passport and/or utility bill
- Banking details including bank, branch, and account number
- Bank statement
- Credit report
- Unique identifier such as username, account number, and password

Ascendant will advise you of the purposes for which personal information is being collected. In some cases, Ascendant may ask for your express consent, such as in the case of conducting credit or background checks. In other cases, your consent may be implied by your acceptance of our terms and agreements or by using a product or service that you have requested.

Ascendant will not routinely collect more information than is necessary to provide you with the products and services you have requested, or as required by law. The information we collect, use, and disclose is for purposes that a reasonable person would consider to be appropriate in the circumstances. We will only collect personal information by means that are fair and lawful and will not mislead you about the purposes for which personal information is collected.

Ascendant may collect, use, or disclose your personal information without your consent only as authorized or required by law. For example, Ascendant may collect, use, or disclose your personal information without your knowledge or consent in exceptional circumstances, including:

- When the information is needed to assist in an emergency that threatens an individual's life or personal safety
- When certain information is publicly available
- When collecting a debt owed to Ascendant
- When the information is necessary for a legal proceeding or investigation into a breach of agreement or contravention of law
- Where information is authorized or required by law or for national security
- Where collection, use or disclosure of information is clearly in the interests of the individual to whom it relates

You may withdraw your consent to the use and disclosure of your personal information at any time unless the information is necessary for Ascendant to meet its legal obligations. Ascendant will respect your decision to withdraw consent, however, we may not be able to provide you with certain products and services.

When you access an Ascendant website (www.ascendant.world/), we may collect information about your computer and the internet settings you are using to connect to our site.

IV.3 Disclosure to Third Parties

No personal information will be disclosed to anyone outside Ascendant, except for everyday business purposes and for the same reasons we collected your information such as to process your transactions, manage your account(s), perform information technology functions, respond to lawful government requests, investigations, or court orders, or to offer you products or services:

- To our service providers who perform services on our behalf, such as data processing and storage, fraud prevention and detection, regulatory compliance, bank services and treasury management and payment functions
- Where you have provided us with your consent
- To obtain legal advice from a lawyer
- As permitted or required by law or for national security
- For the purpose of selling all or part of the business or to assess or complete the purchase of new businesses
- As otherwise specified within this policy

Ascendant protects the privacy and security of your information through contractual agreements and by other means, following the same rules as outlined in the DPF Principles, to ensure that other parties to whom personal information is provided protect your personal information in a manner that meets or exceeds Ascendant's own privacy and security provisions. If one of these companies mishandles your information, Ascendant is still responsible unless we can prove we are not at fault according to the DPF Principles.

To provide you with services, your personal information may be provided to service providers, suppliers or agents located inside and outside the United States. Where required by law, your personal information may be provided to government agencies, courts, regulators, and law enforcement agencies located in other jurisdictions.

If we ever were to engage in any onward transfers of your data with third parties for a purpose other than which it was originally collected or subsequently authorized, we would provide you with an opt-out choice to limit the use and disclosure of your personal data.

In cases of onward transfer to third parties of data of EU individuals received pursuant to the EU-U.S. DPF, Ascendant is potentially liable.

In certain situations, Ascendant may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

IV.4 Accessing Your Personal Information

As a client of Ascendant, you have a right of access to your own personal information, subject to certain exceptions. Ascendant will inform you of what personal information it holds about you, how it has been used and where applicable to whom it has been disclosed. Personal information will be made available in a format for clients with a sensory disability. Clients who seeks access, or who seek to correct, amend, delete inaccurate data, or limit the use and disclosure of data, should direct their query to privacy@ascendant.world. If requested to remove data, we will respond within a reasonable timeframe.

This information will be provided to you at no or minimal cost. Where costs for access to your personal information may occur, Ascendant will notify you in advance of those costs and wait for your consent to proceed with the request.

In some instances, we may not be able to provide information about you from our records if the records contain references to other persons, are subject to legal privilege, contain confidential information proprietary to Ascendant, relate to an investigation of a breach of agreement or contravention of laws, or cannot be disclosed for other legal reasons. Where possible, we will attempt to remove the information listed above from the records and provide those records to you in a modified format.

Ascendant will make this information available to you within 30 days of your request unless providing information to you within that period would unreasonably interfere with business operations or restrict our ability to seek expert advice or convert information to a format that provides accessibility to the requested information.

When information is not provided within 30 days, Ascendant will notify you in writing that an extension has been taken, the reasons for the extension, and your ability to challenge the basis of the extension.

If a request is refused, in whole or in part, Ascendant will notify you of the reasons for the refusal.

IV.5 Protection of Personal Information

Ascendant is committed to protecting the personal information you provide to us, and preventing its loss, theft, access, disclosure, duplication, use or modification without your authorization.

Appropriate security measures will be employed based on the sensitivity of personal information. We maintain physical, organizational, and electronic security measures to protect your personal information. These include the use of locked physical locations, limited access to personal information by employees and contractors, and the use of passwords and encryption technologies.

We will use appropriate security measures when disposing of your personal information.

Employees are aware that personal information must be kept confidential, and all employees receive appropriate training to ensure that safeguards are maintained. Personal information is accessed by

employees for the specific purpose of performing their work functions, and all employees abide by our Code of Ethics that includes obligations of confidentiality and privacy.

All our service providers and partners are bound to maintain the confidentiality of your personal information under contract, and not use your personal information for any unauthorized purposes.

Unfortunately, personal information that is transmitted using email is not fully secure and Ascendant cannot guarantee the security of personal information sent using email. Ascendant is not responsible for any damages suffered when you send personal information through email or when we send personal information through email at your request. Once we receive your information, your orders for foreign exchange transfers or money transfers are placed over a secure connection and encrypted.

IV.6 Privacy Enquiries and Complaints

In compliance with the EU-U.S. DPF, Ascendant commits to resolve complaints about our collection or use of your personal information transferred to the U.S. pursuant to the EU-U.S. DPF. EU individuals with inquiries or complaints should first contact Ascendant at:

Office of the Chief Compliance Officer
St. Andrew's Square
Suite 514, 737 Yates Street
Victoria, British Columbia
Canada V8W1L6
privacy@ascendant.world

Ascendant has further committed to refer unresolved DPF Principles-related complaints to a U.S.-based independent dispute resolution mechanism, BBB NATIONAL PROGRAMS. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit www.bbbprograms.org/dpf-complaints more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See **www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf** .

The Federal Trade Commission has jurisdiction over Ascendant's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF).

IV.7 Change of Privacy Policy

From time to time, Ascendant may update this policy. We encourage you to check back to this page on a regular basis to take notice of any changes. This policy was last updated on January 9, 2024.