PRIVACY POLICY

Last Revised: 05/02/2024

YOUR PRIVACY: OVERVIEW

This privacy policy explains how BaaS, LLC, doing business as FairBorrow™Ai ("FairBorrow™Ai," "we" or "us") collects, uses and discloses information about you when you use our websites, mobile applications, and other online services (collectively, the "Services"), when you visit our offices, attend our events or when you otherwise interact with us as described below. Please note that in some cases we may provide separate or additional privacy notices.

REVISIONS TO THIS PRIVACY POLICY

We may change this policy from time to time. If we make changes, we will notify you by revising the date at the top of this policy, and in some cases, we may provide you with additional notice (such as by adding a statement to our website homepage or by sending an email notification). We encourage you to review this policy frequently to stay informed about our information practices and the choices available to you.

COLLECTION OF PERSONAL INFORMATION

In this Privacy Policy, "personal information" means any information that identifies, relates to, describes, is reasonably capable of being associated with or reasonably can be used to identify an individual or household and other data that is linked to personal information.

The types of personal information we collect about you depend on your interactions with us and are described in more detail below.

Personal Information You Provide Directly to Us

We collect personal information you provide directly to us. For example, we collect information when you create an account to access or use the Services, access, or use any collaboration tools or participate in any interactive features of the Services, send us an email, fill out a form, respond to a survey, comment on a blog, register for or participate in an event, apply for a job, interact with us on social media, enter a promotional drawing, or otherwise communicate with us.

The types of personal information we may collect include your:

- Contact information, such as name, email address, postal address, and phone number; and
- Any other information you choose to provide.

Personal Information We Collect Automatically

We automatically collect personal information when you access or use the Services. The types of information we collect may include:

- **Log Information:** We collect log information about your use of the Services, including your browser type and language, app version, access times, pages viewed, Internet Protocol (IP) address, approximate geographic location, and the webpage or online service you visited before navigating to the Services.
- **Device Information:** We collect information about the mobile device you use to access our mobile applications, including the hardware model, operating system and version, unique device identifiers, and mobile network information.

- **Location Information:** In accordance with your device permissions, we may collect information about the precise location of your device. You may stop the collection of precise location information at any time (see the Your Choices section below for details).
- **Information Collected by Cookies and Other Tracking Technologies:** We and our service providers use various technologies to collect information, including cookies and web beacons (or pixel tags). Cookies are small data files stored on your hard drive or in device memory that help us to, among other things, improve the Services and your experience, see which areas and features of the Services are popular and count visits. Web beacons are clear, electronic images that may be used on the Services or in our emails and help deliver cookies, count visits, understand usage, campaign effectiveness, and determine if an email has been opened and acted upon. For more information, please refer to our Cookie Policy.

Personal Information We Collect from Other Sources

We may also collect personal information from other sources and combine that with information we collect through the Services. For example, we may use information from LinkedIn to update information about you in our contact database.

Personal Information We Derive

We may derive information or draw inferences about you based on the other types of personal information we collect. For example, we may infer your location based on your IP address, or that you are interested in employment or participating in an event based on your browsing behavior on our Services.

Use of Personal Information

We use personal information for various purposes, including to:

- Operate and improve the Services;
- Respond to your questions, comments and requests;
- Provide the information or services you request and send you related information, including confirmations and receipts;
- Send you newsletters and updates;
- Communicate with you about our services, programming and events, and other information we think will be of interest to you;
- Assess job applicants and make hiring decisions;
- Monitor and analyze usage, trends, and activities related to the Services;
- Manage your online account(s) and send you technical notices, updates, security alerts, and support and administrative messages;
- Protect the health, safety, and vital interests of our personnel and others; and
- Notify you about any changes to the Services.

We may process and store your personal information in the United States and other countries, which may have less-protective data protection laws than the region in which you are situated. Please note that this processing, including storage, may involve cross-border transfers of your personal information as described in the "Data Transfers" section below.

Disclosure of Personal Information

We may share your personal information as follows or as otherwise described in this Privacy Policy:

- With vendors, consultants, professional advisors, and other service providers (collectively, "Service Providers") working on our behalf and needing access to your personal information to carry out their work for us. Since our Service Providers are located around the world, please note that these disclosures may involve cross-border transfers of your personal information as described in the "Data Transfers" section below;
- In connection with, or during negotiations of, any merger, sale of FairBorrow™Ai's assets, financing or acquisition of all or a portion of our business to another company;
- In response to a request for information if we believe disclosure is in accordance with, or required by, any applicable law or legal process, including lawful requests by public authorities to meet national security or law enforcement requirements;
- If we believe your actions are inconsistent with our user agreements or policies, or to protect the rights, property, and safety of us or any third party; and
- With your consent or at your direction, including if we notify you that your personal information will be shared in a particular manner and you provide such personal information. We may also share your personal information with third parties when you intentionally direct us to do so or when you use our Services to intentionally interact with third parties. We may also share aggregated or de-identified information, which cannot reasonably be used to identify you.

Please note that any personal information you post in your profile, blogs, listings, public or private groups, forums and any other interactive areas of the Services will be available to other users of those features and, in some cases, may be publicly available.

ADVERTISING AND ANALYTICS SERVICES PROVIDED BY OTHERS

We work with analytics providers to better understand your use of our Services. These providers use cookies, web beacons, and other tracking technologies to collect information about your use of the Services and other websites and applications. We use this information to monitor and analyze your browsing behavior, determine the popularity of certain content on our Services, and improve your experience while using our Services.

DATA SECURITY AND DATA TRANSFERS

Data Security

Although we employ reasonable security measures, the transmission of information via the internet is not completely secure or private. If you have any questions about the security of personal information we collect, please contact: privacy@vincent.attorney.

Data Transfers

For the reasons and purposes set forth in this Privacy Policy, the personal information we collect may be transferred to, stored, or otherwise processed in the United States, Canada, and other locations. We also transfer personal information to service providers that process personal information for us in the United States, Canada, and other locations. (As an example, GoDaddy, our web host, may process information for us in various data center locations. In its 10-K Annual Report filed with the U.S. Securities & Exchange Commission for the period ending December 31, 2020, GoDaddy represented that it has data center locations in the United Stated in the states of Arizona, California, Missouri, Virginia, and New York, as well as international data center locations in the countries of France, Germany, the Netherlands, Singapore, and the United Kingdom.) While in another jurisdiction for processing, your personal information may be accessed by the courts, law enforcement, and national security authorities of that jurisdiction. These jurisdictions may not provide the same level of data protection as your home jurisdiction.

The following is a list of relevant third-party service providers we use and links and other information as to how they use and store your data (if any):

- **GoDaddy, Inc.** This is the Web Host for this website (including all navigable and non-navigable webpages). Relevant privacy information for GoDaddy, Inc., is contained in *Appendix A* of this Privacy Policy (see below) and via GoDaddy's Global Privacy Notice, https://www.godaddy.com/agreements/privacy.
- **Tableau Data Management.** We use Tableau, a third-party data management tool provided online by CData Software, Inc. See its Privacy Policy at https://www.cdata.com/company/legal/privacy/. See also "Cookies," below.
- **Stripe, Inc.** This is our third-party payments provider for customers. See its Privacy Policy at: https://stripe.com/privacy.
- **AuthO by Okta.** This is our secure access/ID authenticator provider. See its Privacy Policy at https://www.okta.com/privacy-policy/.

Children's Privacy

The Services are not intended for children under the age of 18. FairBorrow.ai does not target our Services to children under 18 or knowingly collect information from children under the age of 18.

LINKS TO OTHER WEBSITES AND THIRD-PARTY CONTENT

We may provide links to or embed videos hosted by third-party websites, services, and applications, such as YouTube, which are not operated or controlled by FairBorrow.ai. This Privacy Policy does not apply to third-party services, and we cannot take responsibility for the content, privacy policies, or practices of third-party services. We encourage you to review the privacy policies of any third-party service before providing any information to or through them. The Services may include an activity feed, social media buttons and widgets, such as the Facebook "Like" button or the "Share This" button. Your interactions with these features are governed by the privacy policy of the third-party service that provides the feature.

YOUR CHOICES

You have certain choices with respect to how we treat your personal information, as described below.

Correction

You may review and request modifications to your personal information by contacting us at Support@Support.FairBorrow.Ai.

Marketing Communications

You may opt out of receiving promotional communications from us or request changes to your communication preferences by following the instructions in those communications. If you opt out, we may still send you non-promotional communications, such as those about your account or our ongoing business relations.

Mobile Push Notifications/Alerts

With your consent, we may send promotional and non-promotional push notifications or alerts to your mobile device. You can deactivate these messages at any time by changing the notification settings on your mobile device.

Cookies

Most web browsers are set to accept cookies by default. If you prefer, you can usually set your browser to remove or reject cookies. Please note that if you choose to remove or reject cookies, this could affect the availability and functionality of our Services. We use Tableau Data Management by CData Software, Inc. (see "Data Transfer" above), as our third-party service provider for customers using our service. Tableau will not work if you reject their use of cookies. Therefore, our Services will not work if you reject Tableau's cookies. For more information, please see our Cookie Policy.

INFORMATION FOR EUROPEAN ECONOMIC AREA RESIDENTS

If you are a resident of the European Economic Area (EEA), you have certain rights and protections under applicable law regarding the processing of your personal information. The term "personal information" has the meaning given to it by the European General Data Protection Regulation (GDPR). When we process your personal information as described in this Privacy Policy, we will only do so when we have a legitimate interest in processing your personal information (for example, our legitimate interest in providing the Services, responding to your inquiries, or sending you marketing communications), when the processing

is necessary for the performance of a contract between you and us (for example, to provide you with legal services), when the processing is necessary for compliance with a legal obligation to which we are subject, or when we have your consent to process your personal information. When processing is based on consent, you have the right to revoke such consent at any time. You also have the right to access personal information we hold about you and to ask that your personal information be corrected, erased, or transferred. You may also have the right to object to, or request that we restrict, certain processing. If you would like to exercise any of these rights, you may contact us as indicated below. If you have a concern about our processing of personal information that we are not able to resolve, you have the right to lodge a complaint with the data privacy authority where you reside. For contact details of your local Data Protection Authority, please see: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm.

See further, links to the

INFORMATION FOR CALIFORNIA CONSUMERS: YOUR CALIFORNIA PRIVACY RIGHTS

Additional Disclosures Related to Collection, Use, and Disclosure of Personal Information

If you are a California consumer, the California Consumer Privacy Act (CCPA) requires us to disclose the following information with respect to our collection, use, and disclosure of personal information.

Categories of Personal Information Collected: In the preceding 12 months, we have collected the following categories of personal information: identifiers, characteristics of protected classifications under California or U.S. law, professional and employment-related information, education information, commercial information, internet and electronic network activity, inferences drawn about your preferences, and other categories of personal information that relates to or is reasonably capable of being associated with you. For examples of the precise data points we collect, please see "Collection of Personal Information" above.

Business or Commercial Purpose for Collecting and Using Data: We collect personal information for the business or commercial purposes described in the "Use of Personal Information" section above.

Categories of Sources of Personal Information: We collect personal information from you and the sources described in the *"Personal Information We Collect from Other Sources"* section above.

Categories of Personal Information Disclosed and Categories of Third-Party Recipients: In the preceding 12 months, we have disclosed identifiers, commercial information, and internet and electronic network activity with the following categories of recipients: cloud service providers, consultants, data analytics providers, internet service providers, data storage providers, and operating systems and platforms.

Sale of Personal Information (as defined by the CCPA): We do not sell the personal information we collect.

Your Consumer Rights as a California Consumer

Subject to certain limitations, you have the right to request to know more about the categories and pieces of personal information we collect, use, and disclose and to request deletion of their personal information. You also have the right to opt out of sales of personal information, if applicable, and to not be discriminated against for exercising their rights under the CCPA. You may make a rights request by calling 01.425.444.0545 or emailing Support@Support.FairBorrow.Ai. We will verify your request by asking for information sufficient to confirm your identity, such as your name, email address, and information about your interactions with us. If you would like to use an authorized agent registered with the California Secretary of State to exercise your rights, we may request evidence that you have provided such agent with power of attorney or that the agent otherwise has valid written authority to submit requests on your behalf. We will not discriminate against you if you choose to exercise your rights under the CCPA.

CONTACT US

If you have any questions or comments about this Privacy Policy, you may call us at 01.425.444.0545 or email Support@Support.FairBorrow.Ai

APPENDIX A OF PRIVACY POLICY

GoDaddy (Web Host) Statement

Pages 46-48 of Form 10-K dated December 31, 2023, of GoDaddy Inc., a Delaware corporation, 2155 E. GoDaddy Way, Tempe, Arizona 85284, https://www.sec.gov/ix?doc=/Archives/edgar/data/1609711/000160971124000022/gddy-20231231.htm, states as follows:

We are subject to governmental regulation and other legal obligations, particularly related to privacy, data and information security and cybersecurity. Our failure to comply with these or any future laws, regulations or obligations could subject us to sanctions and damages and could harm our reputation and business.

We are subject to a variety of laws and regulations, including regulation by various federal government agencies, including the FTC, FCC and state and local agencies, as well as privacy, data protection and cybersecurity laws in jurisdictions outside of the U.S. We collect personal, sensitive and confidential information, including payment card information from our current and prospective customers, website users and employees. The U.S. federal and various U.S. state and foreign governments have adopted or proposed limitations on, or requirements regarding, the collection, distribution, use, security and storage of personal, sensitive and confidential information, including payment card information, and the FTC and many state attorneys general are applying federal and state consumer protection laws to impose standards on the online collection, use and dissemination of personal, sensitive and confidential information, including payment card information. Self-regulatory obligations, other industry standards, policies and other legal obligations may apply to our collection, distribution, use, security or storage of personal, sensitive and confidential information, including payment card information. These obligations may be interpreted and applied inconsistently from one jurisdiction to another and may conflict with one another, other regulatory requirements or our internal practices. Any failure or perceived failure by us to comply with U.S., E.U. or other foreign privacy or security laws, policies, industry standards or legal obligations or any security incident resulting in the unauthorized access to, or acquisition, release or transfer of, personal, sensitive and confidential information, including payment card information of our customers, employees or others, may result in governmental enforcement actions, litigation, fines and penalties or adverse publicity and could cause our customers to lose trust in us, which could have an adverse effect on our reputation and business.

We expect there will continue to be newly enacted and proposed laws and regulations as well as emerging industry standards concerning privacy, data protection, cybersecurity and AI in the U.S., the E.U. and other jurisdictions, and we cannot yet determine the impact such future laws, regulations and standards may have on our business. Such laws, regulations, standards and other obligations could impair our ability to, or the manner in which we, collect or use information to target advertising to our customers, thereby having a negative impact on our ability to maintain and grow our total customers and increase revenue. For example, California enacted the California Consumer Protection Act, as amended by the California Privacy Rights Act (CPRA, and collectively, CCPA) that, among other things, requires covered companies to provide certain disclosures to California residents and afford such residents certain rights, including the right to opt-out of the sale or sharing of their personal information, or opt-into certain financial incentive programs. Several other states have enacted, and others are considering enacting, similar data privacy and cybersecurity laws that may require disclosures or notices to consumers and the recognition of certain rights relating to personal information, any of which may require us to modify our data processing practices in the future, for which the cost and impact are currently not predictable. Future restrictions on the collection, use, sharing or disclosure of our users' data or additional requirements for express or implied consent of users for the use, disclosure or other processing of such information could increase our operating expenses, require us to modify our products, possibly in a material manner, or stop offering certain products, and could limit our ability to develop and implement new product features.

In particular, with regard to transfers to the U.S. of personal data (as such term is used in the GDPR and applicable E.U. member state legislation, and as similarly defined under the proposed ePrivacy Regulation) from our employees based in Europe and European customers and users, we historically relied upon the E.U.-U.S. Privacy Shield, as well as E.U. Model Clauses in certain circumstances. The E.U.-U.S. Privacy Shield was invalidated by the Court of Justice of the E.U. (CJEU) in July 2020 (Schrems II), and the E.U. Model Clauses have been subject to legal challenge and were updated in June 2021. Following Schrems II, we have an ongoing process to utilize Data Processing Agreements with our customers and vendors, where there is a transfer involving a third country, to incorporate other data transfer mechanisms, such as the 2021 Standard Contractual Clauses (SCCs), for personal data transfers between E.U. and non-E.U. countries without an adequacy decision from the European Commission. We will continue to transfer personal data pursuant to the SCCs, but the CJEA has indicated that sole reliance on SCCs for transfers of personal information outside the European Economic Area may not be sufficient in all circumstances and the transfers must be assessed on a case-by-case basis.

On July 10, 2023, the European Commission's adequacy decision for the E.U.-U.S. Data Privacy Framework (DPF) entered into effect and the E.U.-U.S. DPF Principles (DPF Principles) entered into effect the same date. The DPF and the DPF Principles provide a new mechanism for transferring personal data from the European Economic Area (EEA) to the U.S., with the European Commission having determined that data transfers to the U.S. made by companies who have self-certified their adherence to the DPF and DPF Principles provides a level of data protection comparable to the protection offered in the E.U. However, this decision is facing legal challenges and ultimately may be invalidated by the CJEU just as was the E.U.-U.S. Privacy Shield. On July 17, 2023, the U.S. Department of Commerce recognized several GoDaddy entities, including Go Daddy Operating Company, LLC, as having self-certified their adherence to the DPF by virtue of their prior self-certification under the E.U.-U.S. Privacy Shield. We have updated our global privacy notice and certain other documents, as required by the DPF. If the E.U.-U.S. DPF is invalidated or it is determined

that we are not eligible to continue to transfer personal data pursuant to the DPF, we intend to continue to rely upon the 2021 SCCs as an alternative transfer mechanism. In addition, the UK and the U.S. recently entered into an agreement regarding an extension of the E.U.-U.S. Data Privacy Framework to provide a new mechanism for transfer of personal data from the UK to the U.S., which is described as the UK-U.S. Data Bridge. We have self-certified our compliance with the UK-U.S. Data Bridge. If the UK-U.S. DPF is invalidated or it is determined that we are not eligible to continue to transfer personal information pursuant to the DPF, we intend to continue to rely upon the UK International Data Transfer Agreement for transfers of personal data from the UK to the U.S. Our failure or inability to comply with all requirements of the DPF or a challenge to our use of the 2021 SCCs could limit our ability to transfer data from the E.U., EEA, and UK to the U.S. However, we continue to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated herewith.

Notwithstanding the aforementioned measures, we may be unable to maintain legitimate means for our transfer and receipt of personal data from the E.U. and the EEA. We may, in addition to other impacts, experience additional costs associated with increased compliance burdens, and we and our customers face the potential for regulators in the EEA to apply different standards to the transfer of personal data from the EEA to the U.S., and to block, or require ad hoc verification of measures taken with respect to certain data flows from the EEA to the U.S. We also may be required to engage in new contract negotiations with third parties that aid in processing data on our behalf. We may experience reluctance or refusal by current or prospective European customers to use our products, and we may find it necessary or desirable to make further changes to our handling of personal data of EEA residents. The regulatory environment applicable to the handling of EEA residents' personal data, and our actions taken in response, may cause us to assume additional liabilities or incur additional costs and could result in our business, operating results and financial condition being harmed. Additionally, we and our customers may face a risk of enforcement actions by data protection authorities in the EEA relating to personal data transfers to us and by us from the EEA. Any such enforcement actions could result in substantial costs and diversion of resources, distract management and technical personnel and negatively affect our business, operating results and financial condition.

In addition, several other foreign countries and governmental bodies have laws and regulations concerning the collection, use, transfer and other processing of their residents' personal information, including payment card information, which are often more restrictive than those in the U.S. Although we believe we comply with those laws and regulations applicable to us, these obligations may be modified and interpreted in different ways by courts, and new laws and regulations may be enacted in the future. Within the EEA, the GDPR took full effect on May 25, 2018, and became directly applicable to companies established across E.U. member states. As the GDPR is a regulation rather than a directive, it applies throughout the EEA, but permits member states to enact certain supplemental requirements if they so choose. The GDPR also has broad extraterritorial effect on companies established outside the EEA, with stringent requirements for processors and controllers of personal data, and imposes significant penalties for non-compliance. Noncompliance with the GDPR can trigger fines of up to the greater of €20 million or 4% of global annual revenues. The UK exited the E.U. effective January 31, 2020, which has created uncertainty with regard to the regulation of data protection in the UK. In June 2021, the European Commission adopted an adequacy decision for data transfers from the E.U. to the UK. Nevertheless, this adequacy decision may be revisited and it remains to be seen how the UK's withdrawal from the E.U. will impact the manner in which UK data protection laws or regulations will develop and how data transfers to and from the UK will be regulated and enforced by the UK Information Commissioner's Office, E.U. data protection authorities, or other regulatory bodies in the longer term. In addition, some countries, such as India, are considering or have enacted legislation requiring local storage and processing of data that could increase the cost and complexity of delivering our services.

On October 27, 2022, the E.U. published the Digital Services Act (DSA) in its Official Journal. The DSA, which requires governed companies to comply with its provisions beginning the first quarter of 2024, imposes new content moderation obligations, notice obligations, advertising restrictions and other requirements on digital intermediaries, including providers of intermediary services, hosting services and online platforms, which will cover certain products and services provided by the company and affiliate brands operating within the E.U. Noncompliance with the DSA could result in fines of up to 6% of annual global revenues, which are in addition to the ability of civil society organizations and non-governmental organizations to lodge class action lawsuits.

Any new laws, regulations, other legal obligations or industry standards, or any changed interpretation of existing laws, regulations or other standards may require us to incur additional costs and restrict our business operations. For example, many jurisdictions have enacted laws requiring companies to notify individuals of cybersecurity breaches involving certain types of personal data. These mandatory disclosures regarding a security breach, or any other disclosures we may choose to undertake, could result in an increased risk of litigation and/or negative publicity to us, which may cause our customers to lose confidence in the effectiveness of our cybersecurity measures which could impact our operating results. In addition, we are required under the GDPR and other privacy laws (including the UK version of the GDPR and U.S. state privacy laws) to respond to certain customers' data subject access requests (DSARs), each within a certain time period, which can entail responding to requests to know, access, correct, delete or transfer personal information we process. We may also be required to disclose what specific data we disclose or sell to, or share with, third parties. We are also required under the GDPR and other data privacy laws (including the UK version of the GDPR and U.S. state privacy laws) to honor certain customers' requests relating to our use of customers' personal information for marketing and advertising purposes. We may dedicate significant resources to responding to our customers' DSARs, which could have a negative impact on our operating results. In addition, a failure to respond to DSARs properly could result in fines, negative publicity and damage to our business.

If our privacy or cybersecurity measures fail to comply with current or future laws, regulations, policies, legal obligations or industry standards, or are perceived to have done so, we have in the past been, and may be in the future, subject to litigation and/or regulatory investigations (including the FTC investigation discussed above), and may incur fines or other liabilities, as well as negative publicity and a potential loss of business. Moreover, if future laws, regulations, other legal obligations or industry standards, or any changed interpretations of the foregoing, limit our customers' ability to use and share personal information, including payment card information, or our ability to store, process and share such personal information or other data, demand for our products could decrease, our costs could increase and our business, operating results and financial condition could be harmed.