TIFIN Privacy Notice

General

We at The TIFIN Group LLC ("TIFIN Group" and together with its subsidiaries and affiliates and the respective businesses of each, collectively, the "Company Group" and each such company, a "Company") value the privacy of individuals and companies who use the Company Group's websites, platforms and services (collectively, "Services"). This privacy notice (this "Privacy Notice") explains how the Company Group collects, uses and discloses personal information from users of Company Group Services ("you" or "your"). As used herein "personal information" or "Personal Information" means any information relating to an identified or identifiable individual. By using the Services, you agree to the collection, use, disclosure and procedures described in this Privacy Notice. Please note that your use of the Services is also subject to the Company Group Terms of Service (as may be from time to time supplemented or replaced by an individual Company).

1. Personal Information We Collect

The Company Group may collect a variety of Personal Information from or about you or your devices from various sources, as described below.

If you do not provide your Personal Information when requested, you may not be able to use Company Group Services if that information is necessary to provide you with Company Group Services or if the Company Group is legally required to collect it.

a. Personal Information You, your Employer or Business Affiliates Provide to Us

i. **Registration and Profile Information**. When you create an account to use Company Group Services, a Company will ask you for certain Personal Information including without limitation your name, address, phone number, email address, DOB, SSN, company name and title.

ii. **Use of Our Services**. When you use Company Group Services, the Company Group will collect and may otherwise process any Personal Information you provide or make available to us via Company Group Services.

iii. **Communications**. If you contact a Company directly, the Company Group will receive certain Personal Information about you. For example, when you contact a Company for more information about one of Company Group platforms, it may receive your name, email address, the contents of a message or attachments that you send to it and other information you choose to provide.

iv. **Employer and Business Affiliates**. Your employer (together with

affiliates "Employer") or a business affiliate of you or Employer may provide us with personal information including without limitation name, address, phone number, email address, DOB, SSN, company name and title.

v. **Careers**. If you decide that you wish to apply for a job with a Company, you may submit your contact information and your resume online. The Company Group will collect the information you choose to provide on your resume, such as your education and employment experience. You may also apply through a third-party platform, such as LinkedIn. If you do so, the Company Group will collect any information you make available to us via such platforms.

b. Personal Information We Collect When You Use Our Services

i. **Location Information**. When you use Company Group Services, it may infer your general location information, for example, by using your internet protocol (IP) address.

ii. **Device Information**. The Company Group will receive information about the device and software you use to access Company Group Services, including IP address, web browser type, operating system version, and application installations.

iii. **Usage Information**. To help us understand how you use Company Group Services and to help us improve them, the Company Group will receive information about your interactions with Company Group Services like the pages or other content you view and the dates and times of your visits.

iv. **Information from Cookies and Similar Technologies**. The Company Group and its third-party partners collect Personal Information using cookies, which are small files of letters and numbers that are stored on your browser or the hard drive of your computer. They contain information that is transferred to your computer's hard drive. The Company Group and its third-party partners also use pixel tags and web beacons on Company Group Services. These are tiny graphic images placed on web pages or in Company Group emails that allow us to determine whether you have performed a specific action. The Company Group uses cookies, beacons, invisible tags, and similar technologies (collectively "**Cookies**") to collect information about your browsing activities and to distinguish you from other users of Company Group Services. This aids your experience when you use Company Group Services and allows us to improve the functionality of Company Group Services. Cookies can be used for performance management (i.e., collecting information on how Company Group Services are being used for analytics purposes). The types of Cookies the Company Group and

third parties use to collect information include: (i) **Strictly Necessary Cookies** — some Cookies are strictly necessary to make Company Group Services available to you and (ii) **Analytical or Performance Cookies** — Cookies for website analytics purposes to operate, maintain and improve Company Group Services, either using our own analytics Cookies or those of third-party analytics providers. Please review your web browser's "Help" file to learn how you may modify your cookie settings. Please note that if you delete or choose not to accept Cookies from Company Group Services, you may not be able to utilize the features of Company Group Services to their fullest potential.

c. Information We Receive from Third Parties. If you choose to link Company Group Services to a third-party account, the Company Group may receive information about you from such account, including without limitation your profile information, your photo, address, phone number, email address, employment/payment/benefit information, or financial or other information provided to such third-party account including your use of such third-party account.

2. How We Use the Personal Information We Collect

The Company Group uses the Personal Information it collects as set forth below.

- To provide, maintain, improve and enhance Company Group Services;
- To personalize your experience on Company Group Services such as by providing tailored content and recommendations;
- To understand and analyze how you use Company Group Services and develop new products, services, features, and functionality;
- To communicate with you, provide you with updates and other information relating to Company Group Services, provide information that you request, respond to comments and questions, and otherwise provide customer support;
- For marketing and advertising purposes, such as developing and providing promotional and advertising materials that may be relevant, valuable, or otherwise of interest to you;
- To generate deidentified or aggregated data for lawful purposes;
- To find and prevent fraud and abuse, and respond to trust and safety issues that may arise;
- For compliance purposes, including enforcing our Terms of Service or other legal rights, or as required by applicable laws and regulations or requested by any judicial process or governmental agency; and
- For other purposes for which we provide notice at the time the Personal Information is collected.

3. Legal Bases for Processing European Personal Information

If you are located in the European Economic Area ("**EEA**") or the United Kingdom ("**UK**"), the Company Group only processes your Personal Information when it has a valid "legal basis," including as set forth below.

- **Consent**. The Company Group processes your Personal Information where you have consented to such processing of your Personal Information. For example, it may process your Personal Information to use Cookies where you have consented to such use.
- **Contractual Necessity**. The Company Group processes your Personal Information where required to provide you with the Services. For example, it may need to process your Personal Information to respond to your inquiries or requests.
- **Compliance with a Legal Obligation**. The Company Group processes your Personal Information where it has a legal obligation to do so. For example, the Company Group may process your Personal Information to comply with tax, labor, and accounting obligations.
- **Legitimate Interests**. The Company Group may process your Personal Information where it or a third party have a legitimate interest in processing your Personal Information. Specifically, the Company Group has a legitimate interest in using your Personal Information for product development and internal analytics purposes, and otherwise to improve the safety, security, and performance of Company Group Services. The Company Group only relies on its or a third party's legitimate interests to process your Personal Information when these interests are not overridden by your rights and interests.

4. ***How We Disclose the Personal Information We Collect.*** The Company Group does not disclose Personal Information it collects from or about you except as described below or otherwise disclosed to you at the time of collection.
    - ***a.*** **Affiliates**. The Company Group may disclose any information it receives to and/or among its partners and/or affiliate Companies for any purpose described in this Privacy Notice.
    - ***b.*** **Vendors and Service Providers**. The Company Group discloses information it receives, as reasonably necessary, to vendors and service providers retained in connection with the provision of Company Group Services.
    - ***c.*** **Customers**. When you use Company Group Services as an employee or authorized user of one of our clients ("Clients"), the Company Group will share your Personal Information with such Client to the extent mandated by contractual relationship between such Client and the Company Group.
    - ***d.*** **Analytics Providers**. The Company Group uses analytics to collect and process certain analytics data. These services may also collect information about your use of other websites, apps, and online resources.
    - ***e.*** **Service Partners**. When you use Company Group Services, the Company Group will disclose your Personal Information to third-party partners, such as financial institutions or investment firms where necessary to provide Company Group Services to you or in response to your request.
    - ***f.*** **As Required by Law and Similar Disclosures**. The Company Group will

access, preserve, and disclose your Personal Information if it reasonably determines doing so is required or appropriate to: (a) comply with law enforcement requests and legal process, such as a court order or subpoena; (b) respond to your requests; or (c) protect your, our, or others' rights, property, or safety. For example, the disclosure of your Personal Information may occur if you post any objectionable content on or through Company Group Services.

g. **Merger, Sale, or Other Asset Transfers**. The Company Group may transfer or disclose your Personal Information to service providers, advisors, potential transactional partners, or other third parties in connection with the consideration, negotiation, or completion of a corporate transaction in which the Company Group at large or a constituent Company is acquired by or merged with another company, or sells, liquidates, or transfers all or a portion of its such companies' assets. The use of your information following any of these events will be governed by the provisions of this Privacy Notice in effect at the time the applicable information was collected.

h. **Consent**. The Company Group will also disclose Personal Information from or about you or your devices with your permission.

5. Your Choices

a. **Marketing Emails**. You can unsubscribe from Company Group promotional emails via the link provided in the emails. Even if you opt out of receiving promotional messages from us, you will continue to receive administrative messages from us.

b. **Additional Privacy Rights**. You have the additional rights described below.

- You may request access to the Personal Information the Company Group maintains about you, update, and correct inaccuracies in your Personal Information, restrict or object to the processing of your Personal Information, have your Personal Information anonymized or deleted, as appropriate, or exercise your right to data portability to easily transfer your Personal Information to another company. In addition, you have the right to lodge a complaint with a supervisory authority, including in your country of residence, place of work or where an incident took place.
- You may withdraw any consent you previously provided to us regarding the processing of your Personal Information at any time and free of charge. The Company Group will apply your preferences going forward and this will not affect the lawfulness of the processing before you withdrew your consent.

You may exercise these rights by contacting us using the contact details at the end of this Privacy Notice. Before fulfilling your request, we may ask you to provide reasonable information to verify your identity. Please note that there are

exceptions and limitations to each of these rights, and that while any changes you make will be reflected in active user databases instantly or within a reasonable period of time, the Company Group may retain information for backups, archiving, prevention of fraud and abuse, analytics, satisfaction of legal obligations, or where we otherwise reasonably believe that we have a legitimate reason to do so.

c. **How to Block Cookies**. You can block Cookies by setting your internet browser to block some or all Cookies. However, if you use your browser settings to block all Cookies (including essential Cookies) you may not be able to access all or parts of Company Group Services. By using Company Group Services, you consent to our use of Cookies and our processing of information collected through such Cookies, in accordance with this Privacy Notice. You can withdraw your consent at any time by deleting placed Cookies and disabling Cookies in your browser, or as explained below. You can change your browser settings to block or notify you when you receive a Cookie, delete Cookies, or browse our Services using your browser's anonymous usage setting. Please refer to your browser instructions or help screen to learn more about how to adjust or modify your browser settings. If you do not agree to the Company Group's use of Cookies or similar technologies which store information on your device, you should change your browser settings accordingly. You should understand that some features of Company Group Services may not function properly if you do not accept Cookies or these technologies. Where required by applicable law, you will be asked to consent to certain Cookies and similar technologies before the Company Group uses or install them on your computer or other device.

d. **Do Not Track**. There is no accepted standard on how to respond to Do Not Track signals, and the Company Group does not respond to such signals.

6. ***Data Retention***. The Company Group takes measures to delete your Personal Information or keep it in a form that does not permit identifying you when this Personal Information is no longer necessary for the purposes for which the Company Group processes it unless it is required by law to keep this Personal Information for a longer period. When determining the retention period, the Company Group takes into account various criteria, such as the type of products and services requested by or provided to you, the nature and length of our relationship with you, the impact on the Services provided to you if the Company Group deletes some Personal Information from or about you, mandatory retention periods provided by applicable law, and any relevant statute of limitations. If you receive Services from constituent Companies within the Company Group where such Services are subject to a written agreement for software and/or services (a "Software &

Services Agreement"), your personal information will be deleted by such applicable Company upon the conclusion of the Services term set forth in such Software & Services Agreement.

7. ***Third Parties.*** Company Group Services may contain links to other websites, products or services that the Company Group does not own or operate. The Company Group is not responsible for the privacy practices of these third parties. Please be aware that this Privacy Notice does not apply to your activities on these third-party services or any information you disclose to these third parties. The Company Group encourages you to read privacy policies applicable to such websites, products or services before providing any information to them.

8. ***Security***. The Company Group makes reasonable efforts to protect your Personal Information by using physical and electronic safeguards designed to improve the security of the Personal Information it maintains. However, because no electronic transmission or storage of information can be entirely secure, the Company Group can make no guarantees as to the security or privacy of your Personal Information.

9. ***Children's Privacy.*** The Company Group does not knowingly collect, maintain, or use Personal Information from children under 13 years of age, and no parts of Company Group Services are directed to such children. If you learn that a child has provided us with Personal Information in violation of this Privacy Notice, you may alert us using the contact and notice information set forth below.

10. ***International Visitors.*** The Company Group Services are hosted in the United States ("**U.S.**") and are intended for users located within the U.S. If you choose to use Company Group Services from the EEA, the UK, or other regions of the world with laws governing data collection and use that may differ from U.S. law, then please note that you are transferring your Personal Information outside of those regions to the U.S. for storage and processing. The Company Group may transfer Personal Information from the EEA or the UK to the U.S. and other third countries based on European Commission-approved or UK Government-approved Standard Contractual Clauses, or otherwise in accordance with applicable data protection laws. The Company Group may also transfer your Personal Information from the U.S. to other countries or regions in connection with storage and processing of data, fulfilling your requests, and operating Company Group Services. By providing any information, including Personal Information, on or through Company Group Services, you consent to such transfer, storage, and processing.

11. ***Changes to This Privacy Notice.*** The Company Group will post any adjustments to the Privacy Notice on this page, and the revised version will be effective when it is posted. If the Company Group materially changes the ways in which it uses or discloses Personal Information previously collected from you through Company Group Services, it will notify you through Company Group Services, by email, or other communication.

12. ***Contact, Notice and Related Information***

If you have any questions, comments, or concerns about Company Group processing activities, please email us at privacy@tifin.com or write to us at:

The TIFIN Group LLC
2440 Junction Place, Suite 300
Boulder, CO 80301

Our Data Controller and Chief Data Protection Officer is set forth below:

Ruben Santiago
privacy@tifin.com

Our Chief Privacy Officer is set forth below:
Jason B. Sitomer
privacy@tifin.com

Our Chief Information and Security Officer is set forth below:

Christopher Lietz

security@tifin.com

<u>Regulated Company Addendum</u>

This Addendum is applicable to affiliate Companies that are investment advisors or broker dealers ("Regulated Companies").

Financial institutions such as banks, broker-dealers, investment advisors and their vendors or services providers (collectively "Firms"), including certain of the Companies, are subject to Regulation S-P, which requires Firms to adopt policies and procedures to protect "nonpublic

personal information" about consumers, and to provide customers, no later than the time a customer relationship is established, a clear and conspicuous notice that reflects (i) the policies and procedures adopted by the Firms to protect nonpublic personal information, (ii) the conditions under which nonpublic personal information about consumers will be disclosed to nonaffiliated third parties, and (iii) the methods available to consumers to prevent the sharing of such information with nonaffiliated third parties. Regulation S-P applies only non-public personal information about individuals (i.e. natural persons) who obtain financial products and services primarily for personal, family or household purposes. Regulation S-P does not apply to information about companies or about individuals who obtain financial products or services primarily for business, commercial or agricultural purposes

Regulation S-P requires an initial notice be delivered at the time a customer relationship is established and another notice be delivered annually during the continuation of the customer relationship. "Annually" means at least once in a period of 12 consecutive months.

A Firm must provide a right to "opt out" if the Firm reserves the right to disclose nonpublic personal information about the consumer to unaffiliated third parties, unless (i) the unaffiliated third party is performing servicing or marketing services for the Firm, (ii) the consumer consents to the disclosure or (iii) the disclosure is permitted or required by law.

A "consumer" is defined as an individual who obtains or has obtained a financial product or service from the Firm for personal, family or household purposes. This includes an individual who provides nonpublic personal information to a Firm, even if the individual ultimately does not open an account. An individual who provides only his or her name, address and general areas of investment interest in connection with a request for more information is not a consumer with respect to a Firm.

A "customer" is a consumer who has established a customer relationship with a Firm. A customer relationship is defined in Regulation S-P to mean a continuing relationship between the consumer and a Firm under which the Firm provides financial products and services to the consumer primarily for personal, family or household purposes. A customer relationship is established when a consumer establishes an investment advisory relationship with a Firm.

"Nonpublic personal information" includes nonpublic "personally identifiable financial information", plus any list, description or grouping of customers that is derived from nonpublic personally identifiable financial information, in each case, in the custody of a Regulated Company.

"Personally identifiable financial information" means any information: (i) the consumer provides to a Firm to obtain financial products or services, (ii) about the consumer resulting from a transaction between the consumer and a Firm, or (iii) that a Firm otherwise obtains from the consumer in connection with providing financial products or services to the consumer. Such

information may include information provided on an account application, account balances and transaction information, the fact that the consumer is or has been a customer of a Firm, information relating to services performed for or transactions entered on behalf of customers, and information from consumer reports and any data, list or analyses derived from such nonpublic personal information, in each case, in the custody of a Regulated Company.

Firms that possess consumer report information for business purposes are required to properly safeguard the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. "Consumer Report Information" means any record about an individual (e.g., name, social security number, phone number, email address, etc.), whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report. The definition includes a compilation of such records but does not include information that does not identify individuals, such as aggregate information or blind data. "Consumer Report" is defined in the Fair Credit Reporting Act ("FCRA"), but generally means information from a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, reputation, etc., which is used for the purpose of establishing eligibility for credit, insurance or employment or used for other purposes permitted under the FCRA. A Firm is not required to ensure perfect destruction of consumer report information. Rather, Firms are required to take "reasonable measures" to protect against unauthorized access to or use of the information in connection with its disposal. The SEC has noted that it expects Firms in devising disposal methods to consider the sensitivity of the consumer report information, the nature and size of the entity's operations, the costs and benefits of different disposal methods and relevant technological changes. The SEC also notes that "reasonable measures" are very likely to require elements such as the establishment of policies and procedures governing disposal, as well as appropriate employee training.

Finally, Regulation S-P requires written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer records and information.

Regulated Companies do not share any nonpublic personal information with any nonaffiliated third parties, except in the following circumstances:

- As necessary to provide the service that the client or authorized user has requested or authorized, or to maintain and service the client's or authorized user's account;
- As required by regulatory authorities or law enforcement officials who may have jurisdiction over the Company Group or an individual Regulated Company or as otherwise required by any applicable law; or
- To the extent reasonably necessary to prevent fraud and unauthorized transactions.

Regulated Company employees ("Employees") are prohibited, either during or after termination of their employment, from disclosing nonpublic personal information to any person or entity

outside the Company Group, except under the circumstances described above. Employees are permitted to disclose nonpublic personal information only to other Employees who need to have access to such information to deliver Company Group services to the client or authorized user.

Security of Information

The Company Group restricts access to nonpublic personal information to Employees who need to know such information to provide services to clients and/or authorized users. Any Employee who is authorized to have access to nonpublic personal information is required to keep such information in a secure, locked compartment on a daily basis as of the close of business each day. All electronic or computer files containing such information must be password secured and firewall protected from access by unauthorized persons. Any conversations involving nonpublic personal information, if appropriate at all, must be conducted by Employees in private and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Delivery Requirements

A Company will provide each customer with an initial notice of the Company Group's privacy notice (as may from time to time be supplemented or replaced by such Company) at the time an account is established. If, at any time, the Company adopts material changes to its privacy notice, the Company shall promptly provide each customer with a revised notice reflecting the new privacy policies.

Disposal of Nonpublic Personal Information. The Regulated Companies will shred, deliver to a document destruction firm, or otherwise render illegible hard copies of any customer or consumer nonpublic personal information in its possession when such Regulated Companies deem possession of the information to no longer be necessary.

Nonpublic personal information stored on disk, CD, tape, or other electronic media shall be cleared, purged, declassified, overwritten and/or encrypted in such a manner so that any information contained therein cannot be restored or decrypted. After the electronic media is cleared, purged, declassified, overwritten, or encrypted, the Chief Compliance Officer shall check that the original information is not backed-up or saved on a hard drive, recycle bin, or other memories.

The Chief Compliance Officer shall require that each third-party service provider engaged by the Regulated Companies that necessarily obtains access to customers' nonpublic personal information during the course of their services on behalf of the Firm to adopt comparable policies and procedures relating to the secure disposal of nonpublic personal information.

External Threats

The Chief Compliance Officer has delegated the following responsibilities to the TIFIN Group Chief Information Security Officer with respect to TIFIN Group. With respect to Company

subsidiaries and affiliates of TIFIN Group, the Chief Information Security Officer has delegated some or all of these responsibilities to the applicable divisional product and technical leadership:

- Maintain reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information;
- Maintain reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information;
- Ensure that, to the extent technically feasible, all personal information stored on pre-approved portable devices, such as laptops or tablets, must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible;
- Monitor all computer systems for unauthorized use of or access to personal information; and
- Conduct reviews of all systems that monitor for external threats no less than annually. A report will be maintained by the Chief Compliance Officer as evidence of the annual review.

Additional Procedures for Massachusetts Residents

For the purposes of the procedures in this subsection, "personal information" includes a Massachusetts resident's first and last name and any of the following a) social security number; b) driver's license number; or c) financial account number (e.g. bank, credit card, etc.). To the extent that a client or authorized user is a Massachusetts resident, the Regulated Companies will implement the following procedures:

Any personal information maintained or stored on a mobile device (e.g. laptop or smartphone) will be stored in an encrypted format;

To the extent technically feasible, any personal information transmitted wirelessly or across a public network will be transmitted in an encrypted format; and

The Company Group will take reasonable steps to ensure that its service providers who have access to the personal information of the Company Group's clients and/or authorized users will implement and maintain appropriate security measures for the information.

* * *

—Updated as of February 7, 2025