MAKING AUTHENTIC FRIENDSHIPS, LLC MOBILE APP PRIVACY POLICY

Last modified: November 2020

MAKING AUTHENTIC FRIENDSHIPS, LLC complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. **MAKING AUTHENTIC FRIENDSHIPS, LLC** has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

MAKING AUTHENTIC FRIENDSHIPS, LLC. (”**Company**”,“**We**”, “**Us”, “Our”**) respect your privacy and are committed to protecting it through our compliance with applicable data protection and privacy laws. This Privacy Policy describes

- the types of information we may collect or that you may provide when you purchase, download, install, register with, access, or use the **MAF App** (the “**App**”); and
- our practices for collecting, using, maintaining, protecting, and disclosing that information.

This Policy applies only to information we collect in this App and in email, text, and other electronic communications sent through or in connection with this App (the “Service”).

Introduction

Please read this Policy carefully to understand our policies and practices regarding your personal data and how we will treat it. If you do not agree with our policies and practices, do not download, register with, or use this App. By downloading, registering with, or using this App, you expressly consent to:

- The collection and use of personal information and data as set forth in this Policy;
- the use of cookies (and mobile cookies) (as explained below);

- emails sent to you for account management purposes; and
- emails (of which you may opt-out at any time) sent to notify you of promotions and additional services.

We are self-certified as compliant with the EU-US and Swiss-US Privacy Shield Frameworks, as provided in the EU-US Privacy Policy set forth below. In the event of any conflict or inconsistency with the terms of this Privacy Policy and the terms of the EU-US Privacy Policy, the terms of the EU-US Privacy Policy will control.

This policy may change from time to time. Your continued use of our Service after we make changes is deemed to be acceptance of those changes, so please check the policy periodically for updates.

Information We Collect and How We Collect It

We collect information from and about users of our Service:

- Directly from you when you provide it to us.
- Automatically when you use the App.

Information You Provide to Us

- When you download, register with, or use this App, we may ask you to provide information by which you may be personally identified, such as name, postal address, email address, telephone number, or any other identifier by which you may be contacted online or offline (”**Personal data**”). Personal data is provided to us by means of information that you provide by filling in forms in the App. This includes information provided at the time of registering to use the App, and requesting further services. We may also ask you for information when you report a problem with the App.
- Records and copies of your correspondence (including email addresses and phone numbers), if you contact us.
- Details of transactions you carry out through the App and of the fulfillment of your orders. You may be required to provide financial information before placing an order through the App.
- Your search queries on the App.

Personal Data

When you register for our Services, and in the course of use of the Service, we collect the following:

- First and last name
- business name (if applicable)
- email address
- physical address
- phone number
- time zone

*We do not store or maintain credit card information, rather our vendor/partners do (see below).

You may provide information to be published or displayed (”**Posted**”) on public areas of websites you access through the App (collectively, “**User Contributions**”). Your User Contributions are Posted and transmitted to others at your own risk. Although you may set certain privacy settings for such information by logging into your account profile, please be aware that no security measures are perfect or impenetrable. Additionally, we cannot control the actions of third parties with whom you may choose to share your User Contributions. Therefore, we cannot and do not guarantee that your User Contributions will not be viewed by unauthorized persons.

Excluded Data

We do not solicit and will not knowingly collect data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sexuality; or genetic or biometric data; or data related to criminal convictions or offenses.

Legal Bases for Collection

We collect and use personal data only if supported by a lawful basis. Lawful bases include: (i) consent (if given by you including by your choice to submit such data, which you are free to withdraw at any time); (ii) contract (including the offering and purchase, for a fee or otherwise, of membership in MAF); and (iii) our legitimate interests, including for direct marketing purposes (of which

you may opt-out or object), to perform, maintain and improve the Services, and as further set forth in this Policy.

Retention

We retain Personal Data from closed accounts, if, for as long as, and to the fullest extent permitted by applicable law, including in order to comply with law, prevent fraud, collect any fees owed, resolve disputes, troubleshoot problems, assist with any investigations, enforce our agreements and policies, and take other actions otherwise permitted by law or as specified elsewhere in this Policy.

Automatic Information Collection

When you download, access, and use the App, it may use technology to automatically collect:

- **Usage Details.** When you access and use the App, we may automatically collect certain details of your access to and use of the App, including traffic data, location data, logs, and other communication data and the resources that you access and use on or through the App.
- **Device Information.** We may collect information about your mobile device and internet connection, including the device's unique device identifier, IP address, operating system, browser type, mobile network information, and the device's telephone number.
- **Stored Information and Files.** The App also may access metadata and other information associated with other files stored on your device. This may include, for example, photographs, audio and video clips, personal contacts, and address book information.
- **Location Information.** This App may collect real-time information about the location of your device.

If you do not want us to collect this information, do not download the App or delete it from your device.

We also may use these technologies to collect information about your activities over time and across third-party websites, apps, or other online services (behavioral tracking). You can opt-out of behavioral tracking on or through this app in your user preferences.

Information Collection Technologies. The technologies we use for automatic information collection may include:

- **Cookies (or mobile cookies).** A cookie is a small file placed on your smartphone that may uniquely identify your browser and collect certain information about you. Among other things, cookies help us analyze our web page flow, customize our Service, measure promotional effectiveness, and promote trust and safety. It may be possible to refuse to accept mobile cookies by activating the appropriate setting on your smartphone. However, if you select this setting you may be unable to access certain parts of our App. You may encounter cookies from third parties that we do not control. For more information about cookies and how to refuse them, visit org.

The following is an illustrative list of the cookies that may be used and installed on your computer or device:

Name: access_token

Purpose: A unique identifier given to the user after login used to authorize communication with the system.

Duration: session-only

Source: MAF

Type: functional

Name: client

Purpose: A secondary unique identifier that works with access_token to allow secure communication with the system.

Duration: session-only

Source: MAF

Type: functional

Name: uid

Purpose: Email address of the user, used to identify client-server requests.

Duration: session-only

Source: MAF

Type: functional

- **Web Beacons.** Pages of the App and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those pages or opened an email and for other related app statistics (for example, recording the popularity of certain app content and verifying system and server integrity). These devices are used to collect Non-Personal data, and may be aggregated with similar data collected from other users. We do not use such data in any way to create or maintain Personal data about you.

The usage information we collect helps us to improve our Service and to deliver a better and more personalized experience by enabling us to:

- Estimate our audience size and usage patterns.
- Store information about your preferences, allowing us to customize our App according to your individual interests.
- Speed up your searches.
- Recognize you when you use the App.

We may also use your information to contact you about our own and third parties' goods and services that may be of interest to you. If you do not want us to use your information in this way, you may opt-out at any time by adjusting your user preferences in your account profile.

We may use the information we collect to display advertisements to our advertisers' target audiences. Even though we do not disclose your personal data for these purposes without your consent, if you click on or otherwise interact with an advertisement, the advertiser may assume that you meet its target criteria.

If you reside in the European Union, Switzerland, Norway, Lichtenstein or Iceland (collectively, the "EEA"), and are protected by European data protection requirements, we will treat your information in compliance with our

EU-US Privacy Policy (below). In addition, we are complaint with the EU's General Data Protection Regulation (GDPR).

Disclosure of Your Information

We may disclose aggregated information about our users, and information that does not identify any individual or device, without restriction.

We do not disclose, sell or rent your personal data to third parties for their marketing purposes without your prior consent. If you do consent but later change your mind, you may contact us and we will cease any such activity.

We may disclose personal data, including EEA personal data that we collect or you provide to third parties for the following purposes:

(i) To our subsidiaries and affiliates for the purpose of providing our Service.

(ii) To contractors, service providers, and other third parties we use to support our business and who are bound by contractual obligations to process personal data with equivalent protections to this Policy and use it only for the purposes for which you consent to.

(iii) Under written obligations of confidentiality, to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by Company about our App users is among the assets transferred.

(iv) To fulfill the purpose for which you provide it.

(vi) With your consent.

(vii) To comply with any court order, law, or legal process, including to respond to any government or regulatory request.

(viii) To enforce our rights arising from any contracts entered into between you and us, including the App EULA, and for billing and collection.

(iv) If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of Company, our customers or others. This includes

exchanging information with other companies and organizations for the purposes of fraud protection and credit risk reduction.

Your Rights to Object, Review, Rectify, Erasure, and Portability

You can review and change your personal information by logging into the App and visiting your account profile page.

If at any time you choose to opt out from allowing us to share with or disclose to non-agent third parties your personal information in the future, or if you wish to request access to, or deletion or modification of, any Personal Data that we have about you that we don't already make available to you for your review and deletion or modification, contact us directly via email. We endeavor to provide such data in a portable, structured, commonly-used, and machine-readable format.

We cannot delete your personal information except by also deleting your user account. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement or cause the information to be incorrect. If you delete your User Contributions from the App, copies of your User Contributions may remain viewable in cached and archived pages, or might have been copied or stored by other App users. Proper access and use of information provided on the App, including User Contributions, is governed by our terms of use.

We advise you to promptly update your Personal Data if it changes or is inaccurate. Once you make a public (to the members or otherwise) Content posting, you may not be able to change or remove it. If you deactivate your membership, your profile page (with a notice that your membership has been deactivated) will still be visible and all your Content will still be accessible.

Your Choices About Our Collection, Use, and Disclosure of Your Information

We strive to provide you with choices regarding the personal information you provide to us. This section describes mechanisms we provide for you to control certain uses and disclosures of over your information.

- **Tracking Technologies.** You can set your browser to refuse all or some browser cookies, or to alert you when cookies are being sent. If

you disable or refuse cookies or block the use of other tracking technologies, some parts of the App may then be inaccessible or not function properly.

- **Location Information.** You can choose whether or not to allow the App to collect and use information about your location through the device's privacy settings or by logging into the App and adjusting your user preferences in your account profile by checking or unchecking the relevant boxes. If you block the use of location information, some parts of the App may ben be inaccessible or not function properly.
- **Promotion by the Company.** If you do not want us to use your email address to promote our own or third parties' products or services, you can opt-out by logging into the App and adjusting your user preferences in your account profile by checking or unchecking the relevant boxes.
- **Targeted Advertising by the Company.** If you do not want us to use information that we collect or that you provide to us to deliver advertisements according to our advertisers' target-audience preferences, you can opt-out by logging into the App and adjusting your user advertising preferences in your account profile by checking or unchecking the relevant boxes.
- **Disclosure of Your Information for Third-Party Advertising and Marketing.** If you do not want us to share your personal information with unaffiliated or non-agent third parties for advertising and marketing purposes, you can opt-out by logging into the App and adjusting your user preferences in your account profile by checking or unchecking the relevant boxes.

We do not control third parties' collection or use of your information to serve interest-based advertising. However these third parties may provide you with ways to choose not to have your information collected or used in this way. You can opt out of receiving targeted ads from members of the Network Advertising Initiative ("**NAI**") on the NAI's website.

Your California Privacy Rights

If you are a California resident, California law may provide you with additional rights regarding our use of your personal information.

(i) "Do Not Track" under the California Online Privacy Protection Act (CalOPPA) of 2014. As mentioned above, MAF may use information collection technologies to collect information about your activities over time

and across third-party websites, apps, or other online services (behavioral tracking). You can opt-out of behavioral tracking on or through this app in your user preferences.

(ii) California's "Shine the Light" law (Civil Code Section § 1798.83) permits users of our App that are California residents to request certain information regarding our disclosure of personal information to third parties for their direct marketing purposes.

International Transfers of Personal Data

The App may be hosted on servers located in countries outside of your own country. The laws applicable to the protection of personal data in such countries may be different from those applicable in your home country. In particular, if you are located within the European Union, please note that personal data collected by us is transferred outside the European Union / European Economic Area (EEA).

Data Security

We have implemented measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure. All information you provide to us is stored on our secure servers behind firewalls. Any payment transactions will be encrypted using SSL technology.

The safety and security of your information also depends on you. Where we have given you (or where you have chosen) a password for access to certain parts of our App, you are responsible for keeping this password confidential. We ask you not to share your password with anyone. We urge you to be careful about giving out information in public areas of the App like message boards. The information you share in public areas may be viewed by any user of the App.

Unfortunately, the transmission of information via the internet and mobile platforms is not completely secure. Although we do our best to protect your personal information, we cannot guarantee the security of your personal information transmitted through our App. Any transmission of personal information is at your own risk. We are not responsible for circumvention of any privacy settings or security measures we provide.

Changes to Our Privacy Policy

We may update our privacy policy from time to time. If we make material changes to how we treat our users' personal information, we will post the new privacy policy on this page with a notice that the privacy policy has been updated and send you an in-App alert the first time you use the App after we make the change.

The date the privacy policy was last revised is identified at the top of the page. You are responsible for ensuring we have an up-to-date active and deliverable email address for you and for periodically visiting this privacy policy to check for any changes.

Jurisdiction

MAKING AUTHENTIC FRIENDSHIPS, LLC is located in New York, USA, as are the servers that make the Services available. All matters relating to privacy issues are governed by the laws of the New York and controlling US law. Nothing in this Policy will be construed as an admission or implication that we are subject to the laws or jurisdictions of any national or international jurisdiction or governmental entity, or to non-US law.

EU-US PRIVACY POLICY

This EU-US Privacy Policy explains how we adhere to the privacy principles of the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework with respect to transfers of personal information from the European Union, as well as Norway, Lichtenstein and Iceland (collectively, "EU"), and from Switzerland, to the United States. We are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

The United States Department of Commerce and the European Commission have agreed on a set of Privacy Shield Principles and Supplemental Principles, to enable U.S. companies to satisfy the requirement under European Union law that adequate protection be given to personal information transferred from the EU to the United States (the "EU-US Privacy Shield"). The EU also has recognized the EU-US Privacy Shield as providing adequate data protection. The United States Department of Commerce and the government of Switzerland have agreed on a similar set of Privacy Shield Principles and Supplemental Principles, to enable U.S. companies to satisfy

the requirement under applicable Swiss law that adequate protection be given to personal information transferred from Switzerland to the United States (the "Swiss-US Privacy Shield").

We comply with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. We have certified to the Department of Commerce that we adhere to the Privacy Shield Principles.

A. Scope

This EU-US Privacy Policy applies to all personal information received by us in the United States from the EU and from Switzerland, in any format, including electronic, paper or verbal.B

B. Definitions

For purposes of this Policy, the following definitions will apply:

- "**agent**" means any third party that collects or uses personal information under our instructions and for us, or to which we disclose personal information for use on our behalf.
- "**personal information**" and "**personal data**" means any data, information or data/information set(s) that identifies or could be used by or on behalf of us to identify an individual. Personal information does not include information that is encoded or anonymized, or publicly available information that has not been combined with non-public personal information.
- "**sensitive personal information**" means personal information that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, views or activities, that concerns health or sex life, ideological views or activities, information on social security measures or benefits, or information on criminal or administrative proceedings and sanctions other than in the context of pending proceedings. In addition, we will treat as sensitive personal information any information received from a third party where that third party treats and explicitly identifies the information as sensitive within the same meaning as used here.

C. Privacy Shield Principles

The privacy principles in this EU-US Privacy Policy have been developed based on the Privacy Shield Principles and Supplemental Principles. For purposes of these principles and this section C, the term “EU” includes Switzerland.

(i) *Notice*. Where we collect personal information directly from individuals in the EU, we will inform such individuals about the purposes for which we collect and use personal information about them, the types of non–agent third parties to which we disclose that information, the choices and means, if any, we offer individuals for limiting the use and disclosure of personal information about them, and how to contact us. Notice will be provided in clear and conspicuous language when individuals are first asked to provide personal information, or as soon as practicable thereafter, and in any event before we use or disclose the information for a purpose other than that for which it was originally collected.

Where we receive personal information from our subsidiaries, affiliates or other entities in the EU, we will use and disclose such information in accordance with the notices provided by such entities and the choices made by the individuals to whom such personal information relates.

(ii) *Choice*. We will offer individuals the opportunity to choose (opt-out) whether their personal information is (a) to be disclosed to a non-agent third party, or (b) to be used for a purpose that is materially different than the purpose for which it was originally collected or subsequently authorized by the individual.

For sensitive personal information, we don’t solicit such information and there’s no need to disclose such information in order to use the Service. If we elect in the future to solicit such information, we will give individuals the opportunity to affirmatively and explicitly (opt-in) consent to the disclosure of such solicited information to a non-agent third party or the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

We will provide individuals with reasonable mechanisms to exercise their choices.

(iii) *Data Integrity*. We will use personal information only in ways that are compatible with and relevant to the purposes for which it was collected or subsequently authorized by the individual. We will take reasonable steps to ensure that personal information is reliable to its intended use, accurate, complete, and current. We will remain compliant for as long as we retain personal information. Personal information will be retained in a form identifying or making identifiable an individual only for so long as necessary to process such information, subject to our right to retain such information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis.

(iv) *Accountability for Onward Transfer*. To transfer personal data to an agent, we will: (a) transfer such data only for limited and specified purposes; (b) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Privacy Shield Principles; (c) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with our obligations under the Privacy Shield Principles; (d) require the agent to notify us if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles; (e) upon notice, including under (d), take reasonable and appropriate steps to stop and remediate unauthorized processing; (f) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request; and (g) enter into enforceable contracts with agents consistent with this Policy.

We will undertake to obtain assurances from our agents that they will safeguard personal information consistent with this Policy. Examples of appropriate assurances that may be provided by agents include: (h) a contract obligating the agent to provide at least the same or substantially similar level of protection as is required by the relevant Privacy Shield Principles, (i) such agent being certified as Privacy Shield Principles-compliant, (j) such agent being subject to the EU Data Protection Directive, or (k) such agent being subject to another EU or Swiss adequacy finding (e.g., companies located in Canada). Where we have knowledge that an agent is using or disclosing personal information in a manner contrary to this policy, we will take reasonable steps to prevent or stop such use or disclosure.

(v) *Access and Correction*. Upon request, we will grant individuals reasonable access to personal information that it holds about them. In addition, we will

take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete, or that has been processed in violation of the Privacy Shield Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

(vi) *Security*. We will take reasonable and appropriate measures to protect personal information in our possession from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and nature of the personal data.

(vii) *Enforcement*. We will conduct compliance reviews of our relevant privacy practices to verify adherence to this EU-US Privacy Policy and appropriate employee and agent training as necessary. Any employee or agent of ours that we determine is in violation of this policy will be subject to disciplinary action up to and including termination of employment or service. We will be responsible if our agent processes personal information in a manner inconsistent with the Privacy Shield Principles, unless we prove that we are not responsible for the event giving rise to the damage.

(viii) *Dispute Resolution*. Any questions or concerns regarding the use or disclosure of personal information should be directed to the **MAKING AUTHENTIC FRIENDSHIPS, LLC** Privacy Agent at the address given below. We will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal information by reference to the Privacy Policy and this EU-US Privacy Policy in an expeditious manner, and at no cost to the individual.

We have further committed to refer unresolved Privacy Shield complaints to JAMS (jamsadr.com), an alternative dispute resolution provider located in the United States, which serves as our third-party dispute resolution provider for Privacy Shield Principles-related disputes. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact or visit JAMS for more information or to file a complaint. The services of JAMS are provided at no cost to you.

Individuals may submit complaints on an individualized basis (and not purporting to be acting in a representative capacity or on behalf of a class) to JAMS. No damages, fees, or other remedies are available. Arbitrators will

have the authority only to award individual-specific non-monetary equitable relief (such as access, correction, deletion, or return of the individual data's in question). Each party will bear its own attorneys fees, subject to the rules of JAMS.

In addition, individuals may submit disputes to binding arbitration who first comply with pre-arbitration requirements. Arbitration may not be invoked and is not available if the individual's same claimed violation of the Privacy Shield Principles: (a) has previously been subject to binding arbitration; (b) was the subject of a final judgment entered in a court action to which the individual was a party; or (c) was previously settled by the parties.

D. Limitation

Adherence to this EU-US Privacy Policy is limited to the extent (i) required to respond to a legal or ethical obligation; (ii) necessary to meet national security, public interest or law enforcement obligations; and (iii) expressly permitted by an applicable law, rule or regulation.

E. Privacy Policy

We recognize the importance of maintaining the privacy of information collected online and via applications, and have created the Privacy Policy (of which this EU-US Privacy Policy is a part) governing the treatment of personal information collected through web sites and applications that we operate. The Privacy Policy reflects additional legal requirements and evolving standards with respect to privacy, and in fact, we utilize this Privacy Policy in facilitating adherence to the Privacy Shield Principles. As such, this EU-US Privacy Policy and the Privacy Policy should be construed harmoniously wherever possible; however, with respect to personal information that is transferred from the EU or Switzerland to the US, the Privacy Policy is subordinate to this EU-US Privacy Policyy