End User Terms & Conditions

Version 1.1 - Effective March 6, 2023

Prove Identity, Inc. (hereinafter "**Prove**", "**we**", "**our**", or "**us**") provides digital identity verification and authentication products and services (our "**Solutions**") which are designed to help prevent fraudulent transactions on behalf of our business clients and individuals like you (the "**end user**", "**consumer**", "**you**", or "**yourself**") when you interact online, such as when accessing mobile applications, logging into online accounts, or making digital payments. Our Solutions require the processing of information that either alone, or in combination with other information, can be used to identify you, including, without limitation, your first and last name, residential or mailing address, phone number, social security number or other government-issued number, date of birth, biometric data, IP address, or other data that is personally identifiable as defined under other applicable privacy and data protection laws (your "**Personal Information**"). These *End User Terms & Conditions* (our "**Terms**") aim to help you understand how we collect, use, and share your Personal Information to develop, provide, improve, and protect our Solutions, and as otherwise outlined herein.

Please note that these Terms do not detail what our Clients do with your Personal Information when using our Solutions. For more information on how our Clients use your Personal Information for this type of processing, please contact the third party directly. For more information on Prove's commitment to end user privacy and data protection practices, please review our Privacy Policy.

Our Goal

End user privacy, data protection, and transparency are very important to us. The goal of these Terms is to (i) clearly outline what Personal Information we collect from and about end users like you, and (ii) explain how we use, share, and treat that information for the purposes of (a) preventing fraud for third party application developers (our "**Clients**") and (b) creating and maintaining Prove-managed, tokenized digital identities that power and inform our Solutions.

Information We Collect and Categories of Sources

Prove may collect and further process the Personal Information you provide while using our Clients' applications that integrate our Solutions to help verify your identity and/or authenticate you into our Clients' applications or platforms in real-time. When you provide this information to access an online platform or perform an online transaction, you give us the identifiers on your behalf for future fraud detection and prevention purposes.

Depending on the Solutions you're interacting with, Prove may collect and further process one or more of the following categories of information:

- *Identifiers* that you provide to our Client directly, such as phone number and email address
- *Inferences* that we have derived from the information we have collected, such as your location from your phone number and device IP address

Identifiers: Information You Provide

You share, or you authorize our Client to share, your Personal Information with Prove for the purpose of us verifying your identity and/or authenticating you into the Client application or platform ("**Identifiers**"). This may include Personal Information such as name, address, date of birth, phone number, social security number, and email address.

You authorize Prove to collect and further process those same Identifiers in order to create and maintain secure, tokenized digital identities that can be used during your future online transactions with Client and other third parties to help prevent identity theft and fraudulent transactions. ‘

Inferences: Information We Receive From Your Devices and/or Your Mobile Provider

You authorize Prove to collect and further process other device data when you use your device to connect our services through a Client's application, such as IP address, that allows us to infer things about you such as location ("**Inference Data**").

You authorize your wireless carrier to use or disclose information about your account and your wireless device, if available, to Prove and/or its service provider(s) for the duration of your business relationship, solely to help them identify you or your wireless device and to prevent fraud. This may include Inference Data. See our Privacy Policy for how we treat your data.

How We Use Your Personal Information

We use your Personal Information, including Identifiers and Inference Data, for one or more of the following business purposes:

- **Provide Solutions**: To operate, provide, and maintain our Solutions.
- **Develop Existing Solutions:** To improve, enhance, modify, add to, and further develop our Solutions.
- **Protect Your Security and Privacy:** To help protect you, our Clients, our partners, Prove, and others from fraud, malicious activity, and other privacy and security-related concerns.
- **Develop New Solutions:** To develop new products and services.
- **Provide Support:** To provide customer support to you or to our Clients, including to help respond to your inquiries related to our Solutions or developers' applications.
- **For Legal Purposes:** To comply with contractual or legal obligations under applicable law and for other legal purposes such as to establish and defend against claims.

- **With Your Consent:** For other purposes with your consent or by your direction.

When We Share Your Personal Information

We may share your Personal Information with certain third parties (i.e., Clients, data partners, and other subprocessors) for the purposes outlined below so long as the third party provides at least the same level of data protection as Prove does and only uses your Personal Information for permitted purposes stipulated in our applicable agreements limited to identity verification, user authentication, and fraud prevention:

- **Vendors**: To provide our Solutions, provided such companies protect your information and only use it for the purposes we specify.

- **Business Transfers**: We may share your Personal Information with other parties in connection with a company transaction, such as a merger, sale of company assets or shares, reorganization, financing, change of control or acquisition of all or a portion of our business by another company of a third party, or in the event of a bankruptcy or related or similar proceedings.

- **Legal Requirements**: We may share your Personal Information with law enforcement, regulatory authorities, courts, and governmental agencies to comply with subpoenas or other legal orders, legal or regulatory requirements, and government requests. We may also disclose Personal Information to verify or enforce compliance with other agreements or policies governing our Solutions, applicable laws, rules, and regulations, or whenever we believe disclosure is necessary to limit our legal liability or to protect or enforce the rights, interests, or safety of the Solutions, end users, or other third parties. We reserve the right to report to law enforcement agencies any activities that we, in good faith, believe to be unlawful.

We may also share your Personal Information with others in an aggregated or otherwise anonymized form that does not reasonably identify you directly as an individual.

How We Protect Personal Information

- **Keeping Personal Information Secure.** Prove maintains appropriate administrative, technical, and physical security measures to protect your Personal Information, including controls that prevent the unauthorized access and use of such data. Prove's Information Security Program aligns with security standards such as NIST 800-53 and industry best practices, and has been reviewed by accredited third party auditors.

- **Data Retention.** We retain Personal Information for no longer than necessary to fulfil the purposes for which it was collected and used, as described in these Terms, unless we are

required by law, regulation or for litigation and regulatory investigations to keep it for longer periods of time.

Please see the 'Exercise Your Rights' section of these Terms for more information on the options that are available to you, including the right to request deletion of Personal Information.

International Data Transfers

Prove's global headquarters are in the United States but we have affiliates and vendors that operate around the world to provide our Solutions. Where we transfer your Personal Information to a country that does not provide adequate data protection legislation, we will ensure that it is protected and transferred in a manner consistent with legal requirements applicable to the jurisdiction and classification of information, such as with the EU's Standard Contractual Clauses.

Consumer Privacy Rights (United States)

Several US states have enacted privacy and data protection-related statutes that grant you certain rights in connection with your Personal Information. Your state of residence will determine which rights are available to you. The following section references a sampling of those rights:

California End User Rights

If you are a California resident, the California Consumer Privacy Act (as amended by the California Privacy Rights Act) provides you with certain rights with regards to your Personal Information:

1. **Right to know.** The right to know what Personal Information we have collected, sold, or disclosed about you over the past 12 months.
2. **Right to delete.** The right to request that we delete any Personal Information we've collected about you (subject to certain exceptions).
3. **Right to opt out of sale.** The right to opt out of the (i) sale of your Personal Information and (ii) sharing of your Personal Information for cross-context behavioral advertising.
4. **Right to correction.** The right to correct inaccurate Personal Information we maintain about you.
5. **Right to portability.** The right to portability allows you to easily move, copy, or transfer your Personal Information from one organization to another.
6. **Right to limit the use of sensitive personal information. The right to limit the use of your Sensitive Personal Information (as defined in the statute) to specifically permitted purposes.**

You may make an opt-out or related request by contacting us using the contact information in Section 13 below or clicking the "Do Not Sell My Personal Information" link at the bottom of Prove's website.

Colorado End User Rights

If you are a Colorado resident, the Colorado Privacy Act (CPA) provides you with certain rights with regards to your Personal Information:

1. **Right of access.** The right to confirm we are processing your Personal Information and to access such Personal Information. Please note that the request for additional copies of personal data may result in reasonable fees based on administrative costs.
2. **Right to correction.** The right to correct inaccurate Personal Information.
3. **Right to opt out of sale or targeted advertising.** The right to opt out of the sale of your Personal Information or processing of your Personal Information for targeted advertising purposes.
4. **Right to delete.** The right to request deletion of your personal information.
5. **Right to portability.** The right to portability allows you to easily move, copy, or transfer your Personal Information from one organization to another.
6. **Right to opt out of profiling.** The right to opt out of any profiling activity that furthers a decision producing legal or similarly significant effects for the consumer, including automated decisions.

Connecticut End User Rights

If you are a Connecticut resident, the Connecticut Personal Data Privacy and Online Monitoring Act (CTDPA) provides you with certain rights with regards to your Personal Information:

1. **Right of access.** The right to confirm whether we're processing your Personal Information and to access that Personal Information. Please note that the request for additional copies of personal data may result in reasonable fees based on administrative costs.
2. **Right to correction.** The right to correct inaccurate Personal Information about you.
3. **Right to delete.** The right to have your personal data deleted from our records once we have received and confirmed your verifiable consumer request.
4. **Right to portability.** The right to portability allows you to move, copy or transfer personal data easily from one organization to another.
5. **Right to opt out.** The right to opt out of targeted advertising, the sale of your Personal Information, and profiling leading to decisions that will produce significant legal effects for you.

Utah End User Rights

If you are a Utah resident, the Utah Consumer Privacy Act (UCPA) provides you with certain rights with regards to your Personal Information:

1. **Right of access.** The right to confirm whether we're processing your Personal Information iand to access that Personal Information. Please note that the request for additional copies of personal data may result in reasonable fees based on administrative costs.
2. **Right to delete.** The right to request deletion of the Personal Information you've provided to us.
3. **Right to portability.** The right to portability allows you to easily move, copy, or transfer your Personal Information from one organization to another.
4. **Right to opt out.** The right to opt out of targeted advertising or the sale of your Personal Information.

Virginia End User Rights

If you are a Virginia resident, the Consumer Data Protection Act (CDPA) provides you with certain rights with regards to your Personal Information:

1. **Right of access.** The right to confirm whether we process your Personal Information and to access that Personal Information.
2. **Right to correction.** The right to correct inaccuracies in your Personal Information.
3. **Right to delete.** The right to request deletion of Personal Information provided by or obtained about you.
4. **Right to portability.** The right to obtain a copy of your Personal Information for transmission to another organization.
5. **Right to opt out.** The right to opt out of targeted advertising, the sale of Personal Information, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning you.

Exercising Your Rights

If you wish to exercise any of the rights listed above, you may contact us in writing at the address above or via email at privacy@prove.com at any time, or by visiting the "Exercise Your Rights" page at the bottom of our website. We will comply with applicable laws but may not be able to honor your request in all circumstances.

Exercise Your Rights

Updated March 8, 2023

Prove is committed to protecting the privacy rights of consumers. When you digitally interact with companies that are also Prove's business clients, Prove may be leveraged by those companies to verify your identity and help prevent fraud using your personal information, such as your full name, residential address, email address, mobile telephone number, date of birth, or Social Security Number. Our business clients are responsible for obtaining your consent for and/or giving you legal notice about this processing of your personal information.

Prove uses real-time, secure Application Programming Interface (API) calls to process and protect the personal information transmitted to us from third parties (e.g., our business clients and data partners) as part of our user authentication and identity verification processes. For most of Prove's products and services, Prove does not retain the personal information transmitted to us in real-time by our business clients, but we may retain certain personal data elements from other sources (including consumers directlto help empower our fraud algorithms.

- If you are a resident of the European Union (EU) or the United Kingdom (UK), you may have certain rights under the General Data Protection Regulation ("GDPR") or the UK GDPR to ask Prove to (among other things) rectify inaccurate personal data, erase your personal data, or restrict its processing. Prove will honor these consumer privacy rights, where applicable, as well as similar rights often available for residents of other non-EU countries with data protection and privacy frameworks.
- If you are a resident of California, Colorado, Connecticut, Nevada, Utah, Virginia or other jurisdictions in the United States (US), you may be entitled to various consumer privacy rights, such as the right to opt out from having your personal information shared or used.

Prove will not discriminate against you for exercising your consumer privacy rights. However, before submitting a request to Prove directly, we highly recommend that you first contact the third party company you interacted with (e.g., via their website or mobile app) that uses our services. If you come to us first, we may not be able to fully respond to the request without knowing the identity of the third party company given that we may not store the personal information transmitted to us in real-time from our business clients.

If Prove, on its own or in collaboration with any third party company you've interacted with that shared your personal information with us, is able to successfully address your consumer privacy request (e.g., delete your personal information), please be aware that your personal information may be processed by Prove again in the future if/when you interact with the same company or a different company that is also a Prove business client and re-accept terms that include this type of processing (i.e., you opt-in or consent to processing your data for fraud-related purposes).

Please also note that in addition to helping protect you against fraud, Prove's services make it easier and more convenient for you to interact with companies online and when you dial into call centers. For example, instead of having to answer cumbersome security questions or type in pin codes or passcodes (which can be easily intercepted by fraudsters), Prove's services allow you to be quickly and securely authenticated, enabling you to complete business online and in call centers in a more expeditious manner. By opting out of Prove services, you may lose access to these time-saving and secure benefits.

To exercise your privacy rights, please fill out this form. Once the form has been completed, a member of Prove's Global Privacy team will begin the process of reviewing your submission and contact you with further details.

General Terms & Conditions

Version 1.1 - Effective March 8, 2023

These General Terms and Conditions ("Agreement") set forth the relationship between Prove Identity, Inc., a Delaware corporation with its principal offices at 245 Fifth Avenue, 20th Floor, New York, NY 10016 ("**Prove**") and the individual party listed on the Portal account that is acknowledging this Agreement ("**Developer**") on behalf of its employer and/or another bonafide legal entity listed on the Portal account ("**Client**").

By accepting this Agreement or accessing Prove's Portal and/or Solutions, Developer certifies that it has all necessary rights to agree to the terms of this Agreement, including on behalf of Client. Furthermore, Developer represents and warrants that: (i) it has full legal authority to select a Plan and bind Client to the terms of this Agreement; (ii) Developer has read and understands the legal requirements and restrictions outlined in this Agreement; and (iii) Developer agrees to the terms of this Agreement on behalf of Client.

If Developer does not have the legal authority to bind Client to the terms of this Agreement, Developer shall not accept this Agreement or access the features covered by this Agreement.

This Agreement is effective as of the date of Developer's acknowledgement and, as of that date, Client is considered a party of this Agreement. Prove may update or change the terms of this Agreement at any time at our discretion. If Prove makes any changes deemed to be material in its sole discretion, we will make a reasonable effort to inform you of such change. If you object to a change, your exclusive remedy is to cease any and all access and use of the Portal and Solutions.

1. **DEFINITIONS**

"**Affiliate**" means for any entity, any other entity that, directly or indirectly, Controls, is Controlled by or is under common Control with such entity.

"**Confidential Information**" means any confidential and/or proprietary information or data, in any form, format or media, disclosed by, or accessed or obtained from Disclosing Party (and any notes, summaries, memoranda or other derivatives prepared by the Receiving Party to the extent that they reflect or reveal such confidential and/or proprietary information or data, whether or not such confidential and/or proprietary information or data is marked as "confidential," including, without limitation, (i) information or data that concerns the management, business affairs, relationships, operations, business plans, strategies, forecasts, projects, analyses, pricing,

marketing, sales or financials of the Disclosing Party or its customers or vendors; (ii) information or data that concerns the Disclosing Party's products, services, developments, product concepts, technical and/or platform interfaces, or software (including source and object code); (iii) information or data that concerns the Disclosing Party's methodologies, techniques, designs, drawings, processes procedures, inventions, know-how, pending patents, or Trade Secrets; (iv) any Response Data or Personal Information obtained by either party as a result of this Agreement; (iv) any information or data the Disclosing Party may designate as being confidential, either orally or in writing; (v) any other information or data which, in the normal course of business, would be considered of a confidential nature; and (vi) any copies of the foregoing.

"Control" means, with respect to any entity, the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity, whether through the ownership of voting securities (or other ownership interest), by contract or otherwise.

"Documentation" means the online help files and all other documentation and materials including SDKs (in any format or medium) relating to use of the Solutions and made available by Prove and all modifications to such files, documents or materials as may be updated from time to time.

"**Intellectual Property Rights**" means any and all intellectual property rights and proprietary rights throughout the world and protected under any applicable laws, rules and regulations, whether existing under intellectual property, unfair competition or trade secret laws, or under statute or at common law or equity, including but not limited to: (a) copyrights, trade secrets, trademarks, service marks, trade names, patents, inventions, invention disclosures, know-how, proprietary data and databases, methods, techniques, works of authorship, computer software, systems, change documentation, interfaces, Marks, designs, logos and trade dress, "moral rights," mask works, rights of personality, publicity or privacy, and any other intellectual property and proprietary rights; and (b) any registration, application or right to apply for any of the rights referred to in this clause, including, any pending registrations or applications; and (c) any and all renewals, extensions and restorations thereof, now or hereafter in force and effect. Furthermore, if alternatively reasonable approaches and/or modifications to methodologies, techniques, design details, drawings, processes and procedures, inventions, know-how, pending patents, information disclosures, and/or other intellectual and/or proprietary property is/are reasonably likely to occur to one of ordinary skill in the relevant art, Intellectual Property Rights includes all those alternatively reasonable approaches and/or modifications unless otherwise expressly indicated.

"Marks" means all trademarks, service marks, trade names and logos and other proprietary designations identifying Prove and its products or services.

"Network" means the servers and other equipment on which Prove hosts Solutions.

"Personnel" means a party's employees and contractors, and a party's vendor's employees and contractors.

“**Plan**” means the pay-as-you-go per Transaction model for the Solutions published on the Portal.

“**Portal**” means the webpage where the Developer may access all necessary information related to the Plan, the Documentation and the Solutions on behalf of Client.

“**Processing**” with reference to Personal Information includes collection, use, analysis, modification, deletion, sale, storage, sharing or transfer of such Personal Information.

"**Personal Information**" means, in any form, format or media, (i) any information that either alone, or in combination with other data, can be used to identify an individual, including, without limitation, the individual’s name, address, phone number, social security number or other government-issued number, financial account number, date of birth, address, biometric data (including gait analysis), mother’s maiden name, or other personal information; (ii) any information or data that is personally identifiable as defined under other applicable privacy and data protection laws.

“**Representatives**” means a party’s directors, officers, Affiliates, contractors, consultants, employees, advisors, agents, and any other representatives including legal counsel, accountants, and financial advisors.

“Response Data” means, any information Prove provides to Client and/or Developer in connection with Developer’s or Client’s use of the Solutions with the exception of any information that was initially provided by or on behalf of Client and/or Developer to Prove. Response Data is Prove Confidential Information.

“Security Breach” means (i) any act or omission that compromises the security, confidentiality, availability, and/or integrity of any data or information provided under this Agreement or the physical, technical, administrative or organizational safeguards put in place by Client and/or Developer that relate to the protection of the security, confidentiality or integrity of such data or information provided under this Agreement, or (ii) receipt of a complaint in relation to the privacy, security or data protection practices of Client and/or Developer or a breach or alleged breach of this Agreement relating to Client and/or Developer’s privacy, security and/or data protection practices.

“**Solutions**” means collectively (i) the access Prove provides Developer on behalf of Client to use the Solutions through the Network, which may include access via Graphical User Interfaces (“GUIs”) and portals and/or platforms; (ii) authentication solutions that interoperate with Client’s internal systems in order to provide user authentication for a mobile device application, website or other online service; (iii) the Solutions including data elements and Response Data, ; and (iv) the Documentation..

“Trade Secret” means information, without regard to form, including, but not limited to a formula, pattern, compilation, program, device, method, technique, process or product plans or product information that derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who

might obtain economic value from its disclosure or use; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy; and is information that is considered a Trade Secret under applicable law.

"**Transaction**" means every inquiry Developer, on behalf of Client, sends to Prove for validation.

2. APPOINTMENT AND GRANT OF LICENSE

2.1 License.

2.1.1 Grant. Subject to Developer's continued compliance with all the terms of this Agreement (including all Exhibits attached hereto), Prove hereby grants Client a non-sublicensable, non-transferable, non-exclusive, revocable, restricted license during the Term to (i) access and use the Solutions, including all enhancements, updates and modifications, for Developer's internal use on behalf of Client, in strict accordance with this Agreement. In no event will Client or Developer reproduce, modify, sell, sublicense or otherwise distribute the Solutions as a standalone product or service.

2.1.2 Source Code. No rights are granted to Developer or Client with respect to source code of any component of the Solutions. For clarity, sample code provided as illustrative examples is provided solely as part of the Documentation and is not itself a component of the Solutions.

2.2 License Restrictions. Except as otherwise permitted under this Agreement, Client will not, and will not permit Developer or any third party to:

(i) share, transfer, resell, bundle, rent, distribute, sublicense, or otherwise make the Solutions or Response Data available except as expressly set forth herein and subject to all the controls and protections set forth herein;

(ii) use the Portal or Solutions to send or store infringing or unlawful material;

(iii) send or store viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs via the Portal or Solutions;

(iv) attempt to gain unauthorized access to, or disrupt the integrity or performance of, the Portal or Solutions or the data contained therein;

(v) adapt, modify, translate, copy, disassemble, decompile, reverse engineer, create derivative works of or make any other attempt by any means to discover or obtain the source code or other proprietary information or Response Data;

(vi) access the Portal or Solutions for the purpose of building a competitive product or service or copying its features or user interface for the purpose of reducing the number of transactions under this Agreement;

(vii) use the Portal or Solutions or permit them to be used, for purposes of product evaluation, benchmarking or other comparative analysis intended for publication without Prove's prior written consent;

(viii) use the Response Data for marketing purpose;

(ix) maintain or create any table or database of any kind based on the Response Data for the purpose of avoiding subsequent billable API calls or other service requests to Prove or

(x) use the Portal or Solutions in any way that would violate any applicable federal, state, and local law, court order or regulation.

2.3 Right to Modify Portal or Solutions. Prove may, from time to time in its sole discretion, modify or enhance the Portal, Solutions and/or the Documentation and any such modifications or enhancements provided to Developer hereunder are deemed part of the Portal, Solutions and/or Documentation, as applicable.

2.4 Suspension. Prove, in its sole discretion, may immediately suspend Developer's and Client's right to access and use some or all of the Portal, Solutions, or Response Data if it believes that Client, or Developer on behalf of Client, has i) used the Portal, Solutions or Response Data in an illegal manner, ii) if Developer breaches Sections 6.1 and 6.2 of this Agreement, iii) if Prove reasonably believes that Developer's or Client's use of the Solutions is in violation of the license restrictions set forth in Section 2.1 or 2.2 above or iv) if Client has suffered a Security Breach.

2.5 Reporting by Prove. Developer, on behalf of Client, authorizes Prove to collect, store, host, access, use, reproduce and modify, during and after the Term, any and all data, inputs, responses and other information concerning Client and Developer's use of the Solutions (i) bill Developer for its use of the Solutions (ii) prepare reports for Prove's internal use, (iii) verify Developer's compliance with the terms of this Agreement, (iv) perform or enforce its obligations under this Agreement, and (v) conduct data and usage analytics, parsing routes, data modeling and other analyses as deemed necessary by Prove to test, evaluate, develop and enhance Prove's Solutions, including the creation and management of consumer-based, tokenized digital identities (with the legal consent of each individual consumer which may be collected by Prove directly through the Solutions). In addition, Prove may provide such data, inputs and information on a confidential basis to its technology partners and Affiliates for the purposes described in this Section 2.5.

3. ADDITIONAL DOCUMENTS

The following documents are hereby incorporated into this Agreement by reference:

- Portal Service Level Agreement
- Trademark Guidelines

Prove may update any of the above referenced documents at any time by posting a new version and providing appropriate notice in the Portal.

4. OBLIGATIONS OF CLIENT & DEVELOPER

4.1 Compliance with Certain Laws.

(i) Personal Information. Developer understands that the Solutions may contain other sensitive information governed by certain laws regulating the Processing of Personal Information all of which Developer acknowledges and agrees to comply with on behalf of Client and to ensure that any third parties acting on behalf of Developer or Client also comply. This includes Client and Developer (on behalf of Client) agreeing to provide electronically Prove's End User Terms & Conditions to each individual consumer each time they interact with Prove Solutions through Client's online sites, products, and/or services in order for Prove to obtain and track consumers' consent for their Processing of Personal Information.

4.2 Use of the Solutions.

(i) Developer's use of Prove's APIs, graphical user interfaces, platforms and other access solutions is limited to Developer's access to and use on an authorized and credentialed basis. Developer will not, nor will Client, sublicense any of Prove's Solutions for use by a third party and any attempted sublicensing will be void.

(ii) Storage of Response Data. All Response Data retained by Developer and Client will at all times be maintained in accordance with the confidentiality and information security provisions of the Agreement.

(iii) Liability for Response Data. Prove will have no liability with respect to claims arising from Developer's interpretation or use of the Response Data or decisions and actions allegedly based upon such Response Data.

4.3 No Representations. Neither Developer or Client may make any representations, warranties or guarantees related to the Solutions unless authorized in advance in writing by Prove.

4.4 GLBA and DPPA Requirements. To the extent that Developer or Client receives Response Data that is Personal Information subject to the GLBA and/or the DPPA, and the regulations issued thereunder, Developer and Client acknowledge and agree that each will request, access and use such Solutions solely for the following specific use(s) listed below:

- As necessary to effect, administer, or enforce a transaction requested or authorized by the Consumer;
- To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
- For required institutional risk control, or for resolving consumer disputes or inquiries;
- For use solely in conjunction with a legal or beneficial interest held by Client relating to the Consumer;

- For use solely in Client's fiduciary or representative capacity on behalf of, and with the implied or express consent of, the Consumer;
- To the extent specifically permitted or required under applicable laws other than the GLBA, and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, to self-regulatory organizations, or for an investigation on a matter related to public safety; and/or,
- To comply with applicable federal, state, or local laws, rules, and other applicable legal requirements.

4.5 FCRA Prohibition.

- In relation to Consumers based in the United States, the Client shall not use the Solutions or Response Data to: (i) create a consumer report as defined under 15 USC §1681a ("Consumer Report") or for use by a consumer reporting agency for the purpose of creating a Consumer Report; or (ii) for any other purpose to the extent it would cause Prove to be subject to the Fair Credit Reporting Act ("FCRA") or any similar laws or regulations, or (iii) for any other FCRA permissible purposes;
- Client acknowledges that Prove is a solutions provider and that its performance of its obligations under this Agreement does not fall within the scope of the FCRA. Client undertakes not to provide Prove with Consumer Report data or take any other action which may bring Prove within the scope of the FCRA. If, despite the above, Client's interactions with Prove become subject to the FCRA, Client acknowledges that Prove will act as agent on Client's behalf for the purposes of the FCRA.

4.6 TCPA Prohibition. Client will not use the Solutions to transmit any marketing communications or any communication that would violate any applicable federal, state, and local law, court order or regulation, including but not limited to the Telephone Consumer Protection Act, 47 U.S.C. § 227 ("TCPA"), the rules governing the Do Not Call Registry, currently found at http://www.donotcall.gov, the CAN-SPAM Act, and any other applicable marketing rules in the United States.

4.7 Privacy Requirements. In performing its obligations and exercising its rights under this Agreement, Client will comply with its obligations as a data controller under the applicable data protection and privacy laws. Developer and Client represent that one or both has or will provide notice and consent to its Consumers where legally required under applicable privacy laws including but not limited to the California Consumer Privacy Act ("CCPA") and all other state data protection, privacy, and consumer protections laws in order to receive the Prove Solution. Client will retain such records of notice, and consent where it is legally required, for the duration of this Agreement, plus an additional year unless otherwise required by law.

4.8 Security Requirements.

4.8.1 Securing Personal Information. Client shall treat all Personal Information, as defined in the applicable Agreement, as sensitive and confidential. This includes, but is not limited to securing sensitive files, managing data access, securely disposing of data and paper records and managing devices. Unless otherwise permitted in the Agreement, Client shall not share or

distribute Personal Information with any third party organization or person(s) without the express, written consent of Prove's Legal Department, CFO, or CEO.

4.8.2 Personnel Security. For all Client Personnel who have access to Personal Information, Client shall: (i) Perform background checks that include, at a minimum, national criminal record checks going back seven (7) years, as well as legal identity verification and authentication (e.g., SSN verification); (ii) Require such Personnel to sign an agreement to maintain the confidentiality of such Personal information; (iii) Require such Personnel to be trained on acceptable use of systems, their obligations regarding privacy and data protection laws and their role in the prevention, detection and reporting of security incidents in addition to complying with all other Client security policies; and (iv) Communicate to such employees the relevant aspects of the Information Security Program, including the procedures and penalties for non-compliance. Additionally, Client shall implement a process to terminate access to Personal Information within twenty-four (24) hours upon the termination of Client Personnel.

4.8.3 Information Security Program. Client shall have implemented a documented information security program, policy and standards, and procedures (the "Information Security Program") that is approved by senior management, meets industry best practices, and complies with all applicable regulatory requirements. Client shall internally review the Information Security Program, and all documentation supporting it, at least annually and revise in accordance with changes in industry best practices and/or applicable regulatory requirements. Client shall hire an accredited third party to review its Information Security Program at least annually in order to provide sufficient assurance documentation to Prove upon request or as part of an annual assessment (e.g., SOC 2, Type II report, PCI DSS 3.2 attestation of compliance, ISO 27001 certification, etc.).

4.8.4 Access Controls. All access to Personal Information by Client shall be limited by business need and using the principle of least privilege. All access and actions on Client systems must be attributable to a named individual or a machine process account. Client shall enforce segregation of duties for all development, test, and production environments.

4.8.5 Data Storage and Transmission. All Client systems used to process, transmit, store Personal Information must use strong cryptography controls: a minimum of Transport Layer Security ("TLS") 1.2 for data in transit and at least 256-bit encryption for data at rest. Client shall use Secure File Transfer Protocols ("SFTP") or another equally secure method/ channel when Personal Information is being transferred externally to/from Client. All Personal Information must be encrypted using TLS 1.2 or higher when in transit. If Personal Information is required to be stored on portable storage media or laptop, Client shall ensure that such Personal Information is encrypted with strong cryptography controls (at least 256 bit) and uncompromised technology.

4.8.6 Security Testing and Monitoring. Client shall implement and maintain security configurations, patch management, vulnerability management, and security tooling in line with industry best practices. Client shall test all web applications Processing, transmitting, or storing Personal Information against Open Web Application Security Project ("OWASP") Top ten (10) web application security risks prior to going live and on a regular basis. Client shall conduct

regular penetration testing of internal and external systems that process, transmit, or store Personal Information. Upon written request, Client shall provide Prove with the results of such testing, including summary reports, test details and dates, and information on the progress of remediation related to any findings.

4.8.7 Physical Security. Client shall implement and maintain a clearly defined and documented physical security policy supported by standards that meet industry best practices.

4.8.8 Data Destruction. On expiry or termination of this Agreement, Client shall promptly (and in no case longer than 30 days) and permanently delete all Personal Information, and direct any applicable subcontractor to do the same, unless otherwise approved expressly in writing by Prove's Legal Department, CFO, or CEO. Where Personal Information is required to be retained by Client under applicable laws, this must be notified to Prove prior to the expiry or termination of this agreement with justification provided for its continued retention and anticipated timescales defined for its eventual destruction.

4.8.9 Security Incidents. Client shall document and maintain an Incident Response Plan ("IRP") that is sufficient to comply with applicable data privacy laws. At a minimum, the IRP plan should be tested annually. Client shall document any security event impacting the confidentiality, integrity, or availability of Personal Information ("Security Incident"), including the root cause(s), analysis, and remediation. Client must immediately notify Prove after Client's discovery of any actual or suspected Security Incident, unauthorized disclosure of Response Data or breach of this Agreement by sending an email to incident@prove.com, privacy@prove.com, and legal@prove.com and to the contract notice addressee set forth in Section 13.7 (Notices) of the Agreement by the means set forth therein. Client must provide Prove the following information to the extent such information is known at the time: (i) the nature, root cause and impact of the breach or disclosure; (ii) Client's assessment of immediate risk due to the breach; (iii) corrective actions already taken; (iv) corrective measures to be taken; and (v) notifications made and to be made to regulatory authorities, customers, and consumers. Client must take all reasonable actions to mitigate the effects of such Security Incident or disclosure, including all necessary actions to recover the affected Response Data, and will reasonably cooperate with Prove in connection therewith. Client will not, without the prior written consent of Prove or unless required by law, reference Prove in any notification regarding unauthorized access or disclosure that affects Consumers (a "Breach Notice"). This section is subject to the requirements of state, federal, and local country laws or regulations, including but not limited to any obligation to provide prior notice to law enforcement.

4.8.10 Audit Rights. Client agrees to allow Prove to audit compliance with this Exbibit on a regular basis, but no more once than annually, for at least the length of the engagement ("Annual Reviews"). This may include, as determined by Prove, access to or copies of documentation related to Client's Information Security Program, including but not limited to Client's information security policies and procedures, as well as any recent external, third party assurance documentation (e.g., SOC 2, Type II report, PCI DSS 3.2 attestation of compliance, ISO 27001 certification, etc.).

5 OBLIGATIONS OF PROVE

5.1 Provisioning and Onboarding Service. Provided that Prove has received all fees due under this Agreement from Developer, Prove will provide the Solutions ordered by Developer on behalf of Client in accordance with information received from Developer and the terms and conditions of this Agreement.

5.2 Technical Support. Prove is responsible for providing technical support for the Portal and Solutions to Developer and Client as described in the Portal Service Level Agreement. Prove will not have any support obligations with respect to errors caused by the combination, operation or use of the Solutions with any product not furnished by Prove if such errors would not have resulted from the unmodified, stand-alone Solutions.

Developer Service Level Agreement

1. Definitions. For purposes of this Service Level Agreement ("SLA"), the following terms have the meanings set forth below. All capitalized terms in this SLA that are not defined in this Section 1 or elsewhere in this SLA have the meanings given to them in the General Terms & Conditions.

"**Business Day**" means a day, other than Saturday or Sunday, in which banks are open for business in New York, New York, USA.

"**Defect**" means any failure of the Solutions to operate in any material respect in accordance with the Agreement or relating Documentation.

"**Expected Service Fee for the Month**" means the sum of all Service Fees due to Prove pursuant to the Agreement.

"**Incident**" means any event which is not part of the standard operation of the Solutions and which causes, or may cause, an interruption to, or reduction of, the quality of the Solutions.

"**Normal Business Hours**" means 9:00 AM to 5:00 PM, [Eastern Time], on a Business Day.

"**Response Time**" means the elapsed time from the initial identification of an Incident by Prove or report by Client to Prove and a return call from the technical specialist working on the request to the Client Personnel acknowledging the Incident report with an assigned ticket number and providing a status update.

"**Scheduled Maintenance**" means the performance of tests, upgrades, improvements, preventive maintenance and other similar activities affecting the Solutions which are reasonably likely to cause the Solutions to become unavailable while such activities are being performed or which necessitate the temporary suspension of the Solutions in order for such activities to be performed with reasonable efficiency.

"**Service Availability**" means the percentage of availability of the Solutions in a particular calendar month calculated by the formula:

S = [(T - N) / T] * 100 where S Equals Solution Availability, N equals the number of minutes in which any Solution Outages occurred during the month and T equals the number of minutes in the month less the number of minutes in which Scheduled Maintenance was performed during the month.

"**Solution Outage**" means any condition or set of conditions where the Solutions fail to meet the service levels required under this Exhibit A, except to the extent such condition or set of conditions is caused by circumstances outside of Prove's Span of Control.

"**SLAs**" means the service levels committed to by Prove pursuant to this Exhibit A.

"**Span of Control**" means Prove will be responsible for all Solution Outages and Incidents which include Solutions and the associated provisioning systems which are provided by Prove, not including external connections to MNOs and/or third party data providers or other third-party systems.

"**System**" means the Network.

2. Service Levels.

2.1 Availability of Solutions.

Subject to the terms and conditions of the Agreement, Prove shall provide the real-time API Solutions to Clients with a Solutions Availability of 99.9% exclusive of Scheduled Maintenance and any Incidents that are outside Prove's Span of Control.

The commitment of availability of Solutions is restricted to the Prove System and does not include technical Incidents related to any type of external connection outside of Prove's Span of Control, including Incidents impacting any third party data provider or other third-party system.

Client acknowledges and agrees that Prove cannot guarantee the total reliability of the Solutions which can be subject to, in addition to cases of force majeure events, Client equipment and/or third party software, hardware or network infrastructure failure outside of Prove's data center and not under the direct control of Prove; failure of the external Internet beyond Prove's network; electrical or Internet access disruptions; or attacks (i.e. hacks, denial of service attacks, malicious introduction of viruses and disabling devices) caused by third parties.

2.2 Scheduled Maintenance.

Prove reserves the right to plan Solutions interruptions for Scheduled Maintenance. Prove will plan Scheduled Maintenance when global traffic volumes are or are expected to be low and will use reasonable efforts to adjust the planned dates and/or times for Scheduled Maintenance based on Client's needs. Client will be notified at least five (5) Business Days in advance of Scheduled

Maintenance. Prove will notify Client as soon as practicable upon receipt by Prove of notification from any third party data provider or third party that is processing Client transactions of any third party data provider or third-party maintenance window that will result in downtime of the Solutions.

Prove will provide at least five (5) Business Days prior notification to Client when Scheduled Maintenance of the Solutions are to be expected. Notification will include the starting time, expected duration, and a summary of the changes to be performed during the maintenance period.

2.3 Emergency Maintenance.

Prove may, in its discretion, cause interruptions to the Solutions in the event maintenance or repair of the System is necessary and such maintenance or repair cannot occur as part of Scheduled Maintenance without adversely affecting operation of the Solutions. Prove shall provide Client as much notice as is practicable prior to causing such interruptions. Emergency maintenance resulting in a service impact will be reported as a Service Outage.

2.4 Reporting and Updates.

Prove will monitor and upon request provide Client monthly reporting on Incidents for the period including the total duration of Service Outages, Prove will make commercially reasonable efforts to maintain backward compatibility such that Solutions updates, software Maintenance Releases, and upgrades will be backward compatible with the previous versions of the Solutions. If a change will require losing backward compatibility, it will be communicated to Client three (3) months before that service or API is discontinued, provided that Prove has been afforded such notice of such change. In no circumstances will Client be required to purchase a particular software release, service update, or service upgrades in order to retain backward compatibility to the previous version of Solutions.

2.5 Service Level Credits.

Service Level Credits are Client's sole and exclusive remedy for any violation of these SLAs. The total amount of Service Level Credits awarded in any one-month period will not, under any circumstance, exceed 5% of a Client's cumulative total monthly service fees. Service Level Credits for these SLAs will only be calculated against fees that are calculated on a 'per transaction basis' and for real-time API calls only; fees that are paid on a 'subscription basis' are not eligible for Service Level Credits. If the Solutions Service Availability is less than 99.5% in a calendar month, Client may request a credit on their next invoice equal to the percentage of transactions that failed due to Service Availability falling below 99.5%. For example, if Service Availability fell to 99.4% during January and Client was unable to complete 0.1% of their monthly transactions as a result, Client may request a Service Level Credit equal to 0.1% of their January fees owed to Prove; or, if Service Availability fell to 99% during November and Client was unable to complete 0.2% of their monthly transactions as a result, Client may request a Service Level Credit equal to 0.2% of their November fees owed to Prove.

3. Beta Solution Feedback.

3.1 Beta Solution Feedback.

Recipient shall report to Developer, as soon as practical, any perceived defect in the Product. At the conclusion of the Beta Test, Recipient shall provide to Developer an evaluation of the Product, including both positive and negative aspects. This feedback will be provided through Developer appointed Slack Channel.

4. Support Solutions.

4.1 Software Support.

As Prove develops permanent solutions or fixes for known or potential Defects in the Solutions, it will promptly incorporate them in software Maintenance Releases in a diligent manner. Client will receive the benefit of standard software Maintenance Releases implemented by Prove subject to terms of this Exhibit A. Client will not incur installation costs for software Maintenance Releases.

4.2 Response Times.

In the event of a Defect or Service Outage, Prove will propose within the following time scales a solution, a workaround, or a plan:

Severity Level

1. Critical Priority: (The interface is unavailable to multiple users.)

- Initial target response: Two (2) hours after notification of issue. Target resolution or workaround: 12 hours

2. High Priority: (When specific functions within the interface are not functioning as expected, but the interface itself is available. This also includes when you have difficulty accessing your account.)

- Initial target response: Eight (8) hours from notification of issue. Target resolution or workaround: Within seventy-two (72) hours.

3. Normal Priority: (Standard functionality issues.)

- Initial target response: Within 1 business day after notification Target resolution or workaround: Within five (5) business days.

4.3 Incident Ticket Reporting and Reviewing Process.

Incident ticket review meetings may be arranged upon Client's written request and as agreed between Prove and Client, to track the progress of solving open Incident tickets.

Vendor Data Processing Agreement

This Data Processing Agreement("**DPA**") is entered into by and between Prove Identity, Inc., a Delaware corporation with its principal offices at 245 Fifth Avenue, 20th Floor, New York, NY 10016 and its Affiliates (collectively "**Prove**") and the counterparty listed in the signature block below ("**Vendor**").

WHEREAS, Prove and Vendor have entered into one or more agreements (any such agreement individually or collectively referred to as the "**Master Agreement**") that may require the processing of personal data as described therein.

WHEREAS, this DPA sets out the additional terms, requirements, and conditions on which the parties will obtain, handle, process, disclose, transfer, or store personal data when providing services under the Master Agreement.

NOW, **THEREFORE**, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

"**Affiliates**" means for any entity, any other entity that, directly or indirectly, Controls, is Controlled by or is under common Control with such entity.

"**Confidential Information**" has the same meaning ascribed to it as in the applicable Master Agreement.

"**Consumer**" means a customer of Prove that is a consumer.

"**Control**" means, with respect to any entity, the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity whether through the ownership of voting securities (or other ownership interest), by contract or otherwise.

"**Data Subject**" means an individual who is the subject of the Personal Data and to whom or about the Personal Data relates, directly or indirectly. For the avoidance of doubt, this definition is intended to cover substantially similar terms under applicable Privacy and Data Protection Laws.

"**EEA**" means the European Economic Area.

"**Personal Data**" means any information directly or indirectly linked or associated to a particular identified or identifiable natural person, including but not limited to, names, dates of birth, postal addresses, telephone numbers, electronic mail addresses, social security numbers, and credit card numbers. For the avoidance of doubt, this definition is intended to cover "personal information," "personal data," or substantially similar terms under applicable Privacy and Data Protection Laws.

"**Privacy and Data Protection Laws**" means all applicable laws and regulations relating to the processing, protection, or privacy of Personal Data, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to, the California Consumer Protection Act (CCPA), California Privacy Rights Act (CPRA), Colorado Privacy Act, Virginia Consumer Data Protection Act, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), European General Data Protection Regulation (GDPR), UK GDPR, and Brazilian General Data Protection Law (LGPD).

"**Restricted Transfer**" means the receipt, disclosure, access, transfer, or storage of Personal Data to any person or entity located in:

(i) any country outside the EEA (an "**EEA Restricted Transfer**"); and/or

(ii) any country outside the UK (a "**UK Restricted Transfer**"),

that the applicable supervisory authority has not deemed to provide an adequate level of protection under Privacy and Data Protection Laws.

"**Security Breach**" means any act or omission that compromises the security, confidentiality, integrity, or availability of Services Personal Data or that compromises the physical, technical, administrative, or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure, or acquisition of Services Personal Data is a Security Breach whether or not the incident arises to the level of a security breach under the Privacy and Data Protection Laws.

"**Sensitive Personal Data**" means categories of Personal Data including but not limited to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data used to uniquely identify a natural person, health data, and precise geolocation data. For the avoidance of doubt, this definition in intended to cover "sensitive data," "special categories of personal data," or substantially similar terms under applicable Privacy and Data Protection Laws.

"**Services**" means the services described in the Master Agreement or any other purposes specifically identified in Annex A. This includes "**Solutions**" as that term is defined in the Master Agreement (where applicable).

"**Services Personal Data**" means any Personal Data that Vendor:

(i) obtains, handles, processes, discloses, transfers, or stores on Prove's behalf pursuant to or in connection with the Services ("**Prove Personal Data**"); and/or

(ii) transmits to Prove pursuant to or in connection with the Services.

For the avoidance of doubt, Services Personal Data (including Prove Personal Data) is Confidential Information.

"**Standard Contractual Clauses**" or "**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries as approved by the European Commission (available here). Where applicable, the SCCs may be varied by the UK Transfer Addendum (available here).

"**UK**" means the United Kingdom of Great Britain and Northern Ireland.

1.2 This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Terms not defined in this DPA have the same meaning as the corresponding terms in the Master Agreement.

1.3 The Annexes form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Annexes.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

2.1 Prove and Vendor acknowledge that for the purpose of complying with any applicable Privacy and Data Protection Laws:

(i) Prove is the controller and Vendor is the processor with respect to any Prove Personal Data; and

(ii) Prove and Vendor are joint controllers with respect to any Services Personal Data.

2.2 The party acting as controller with respect to Services Personal Data retains control of such data and remains responsible for its compliance obligations under any applicable Privacy and Data Protection Laws, including providing any required notices and obtaining any required consents, and for processing instructions it gives to the party acting as processor.

2.3 Annex A provides general information regarding processing of Services Personal Data in accordance with this DPA and the Privacy and Data Protection Laws.

3. PROCESSING OBLIGATIONS

3.1 Each party shall only process Services Personal Data to the extent, and in such a manner, as is necessary to perform the Services in accordance with the other party's written instructions. The parties will not process Services Data for any other purpose or in a way that does not comply with this DPA or the Privacy and Data Protection Laws.

3.2 Each party must promptly comply with any request or instruction from the other party to amend, transfer, or delete the Services Personal Data, or to stop, mitigate, or remedy any unauthorized processing.

3.3 Each party shall maintain the confidentiality of all Services Personal Data and shall not disclose Services Personal Data to third parties unless the other party or this DPA specifically authorizes the disclosure or as required by law. If a law requires any party to process or disclose Service Personal Data, such party must first inform the other party of the legal requirement and give that party an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The parties shall reasonably assist one another with meeting any compliance obligations under the Privacy and Data Protection Laws, while also considering the nature of the processing and the information available. For the avoidance of doubt, Prove is not responsible for completing Vendor's privacy impact assessments, data protection impact assessments, transfer impact assessments, or similar requirements; Prove will only provide information or evidence needed to support these compliance activities if it is not already provided in this DPA or otherwise available to Vendor.

4. EMPLOYEE ACCESS TO PERSONAL DATA

4.1 Parties shall limit any Personal Data access based on the principle of least privilege and to:

(i) those employees who require Personal Data access to meet the applicable party's obligations under the Master Agreement; and

(ii) the part or parts of the Personal Data that those employees strictly require for the performance of their duties.

4.2 Parties shall ensure that all employees who have access to Personal Data:

(i) are informed of the Personal Data's confidential nature and use restrictions and are obliged to keep such date confidential.

(ii) have undertaken training on the Privacy and Data Protection Laws relating to the handling of Personal Data and how it applies to their particular duties; and

(iii) are aware of the applicable party's duties and employee's personal duties and obligations under the Privacy and Data Protection Laws and this DPA.

4.3 Each party's employees and contractors ("**Personnel**") who have access to Personal Data shall:

(i) perform background checks that include, at a minimum, national criminal record checks going back seven (7) years, as well as legal identity verification and authorization (e.g., National ID verification);

(ii) require Personnel to sign an agreement to maintain the confidentiality of such Personal Data; and

(iii) require Personnel to be trained on acceptable use of systems, their obligations regarding privacy and data protection laws, and applicable information security policies.

5. SECURITY

5.1 Considering the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each party shall implement appropriate physical, administrative, technical, and organizational measures to ensure a level of security appropriate to the risk of the processing of Personal Data. These measures shall include, at a minimum, the vendor data protection standards set out in Annex D.

5.2 Each party shall immediately notify the other party if it becomes aware of any advance in technology and methods of working which indicate that the parties should adjust their security measures.

5.3 Each party shall take reasonable precautions to preserve the integrity of any Personal Data it processes and to prevent any corruption or loss, including but not limited to establishing effective back-up and data restoration procedures.

6. SECURITY INCIDENT NOTIFICATION AND MANAGEMENT

6.1 Each party shall document and maintain an Incident Response Plan ("**IRP**") which shall be updated and tested at least annually. The IRP shall require that each party document any Security Breach or security event impacting the confidentiality, integrity, or availability of Personal Data (collectively, "**Security Incidents**"). The documentation should contain the root cause(s) of the Security Incident, any analysis conducted internally and by an external forensics firm, and any current or future planned remediation activities.

6.2 Each party shall notify the other party of a Security Incident promptly, but in no event later than 72 hours, upon discovery of such Security Incident.

6.3 Immediately following any Security Incident, the parties will coordinate with each other to investigate the matter. For Security Breaches specifically, the parties will reasonably cooperate in their handling of the matter, including:

(i) assisting with any investigation;

(ii) facilitating interviews with employees, former employees, and others involved in the matter; and

(iii) making available all relevant records, logs, files, data reporting, and other materials required to comply with the Privacy and Data Protection Laws or as otherwise reasonably required by the non-breaching party.

6.4 For Security Incidents involving Prove Personal Data, Prove will determine:

(i) whether and how to provide notice to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation; and

(ii)whether and to what extent to offer any type of remedy to affected Data Subjects.

6.5 For all other Security Incidents, Prove and Vendor will mutually determine:

(i) whether and how to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation; and

(ii) whether and to what extent to offer any type of remedy to affected Data Subjects.

6.6 The party suffering any Security Breach or Security Incident shall cover all reasonable expenses associated with the performance of the obligations under Sections 6.3 to Section 6.5, unless the Security Breach arose from the other party's specific instructions, negligence, willful default, or breach of this DPA, in which case that party will cover all reasonable expenses.

7. SUB-PROCESSORS

7.1 A list of third parties approved to process Prove Personal Data in connection with the provision of the Services (each a "**Sub-processor**") can be provided.

7.2 The parties shall notify one another in writing of any intended change or addition to the Sub-processors and provide the opportunity to object to such change or addition within fourteen (14) days of notification. The party sending notification of any change or addition may cure an objection by:

(i) cancelling its plans to use the Sub-processor with regard to Services Personal Data;

(ii) offering an alternative to fulfill the Services without such Sub-Processor; or

(iii) taking corrective action requested by the objecting party to obtain approval of such Sub-processor.

7.3 Each party shall ensure, and provided evidence upon request, that its Sub-processors:

(i) have entered into a written contract that contains terms that are substantially the same as those set out in this DPA and meet all applicable Privacy and Data Protection Laws; and

(ii) are not authorized to process Services Personal Data for any other purpose than the Services.

7.4 Where a Sub-processor fails to fulfill its obligations under such written contract, the party engaging such Sub-processor remains fully liable to the other party for the Sub-processor's performance of its agreement obligations.

8. RESTRICTED TRANSFERS

8.1 No party shall not make (nor instruct or permit a Sub-processor to make) a Restricted Transfer of any Services Personal Data except with the other party's prior written consent and in accordance with Section 8.2.

8.2 In order to comply with Privacy and Data Protection Laws, the parties agree to incorporate the applicable SCCs as set out in Annex C and take all other actions required to legitimize the transfer, including implementing any needed supplementary measures or supervisory authority consultations.

8.3 The terms of the applicable SCCs shall control to the extent there is any conflict between the applicable SCCs and this DPA.

8.4 If required by any supervisory authority or the applicable Privacy and Data Protection Laws relating to a Restricted Transfer, the parties shall upon request of either party execute or re-execute the applicable SCCs as separate documents if required.

9. COMPLAINTS AND DATA SUBJECT RIGHTS REQUESTS

9.1 Each party must notify the other party promptly if it receives any complaint, notice, or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Privacy and Data Protection Laws.

9.2 Each party must notify the other party within three (3) business days after verifying the identity of a Data Subject of any request to access to their Personal Data or exercise one of the Data Subject's personal data rights.

9.3 Each party shall reasonably cooperate and assist at their own expense in responding to any complaint, notice, communication, or Data Subject request.

9.4 Vendor shall not disclose Services Personal Data to any Data Subject or to another third party without Prove's prior consent unless required to do so by law.

9.5 Prove shall not disclose Services Personal Data to any Data Subject or to another third party without Vendor's prior consent unless required to do so by law.

10. TERM AND TERMINATION

10.1 This DPA shall remain in full force and effect so long as:

(i) the Master Agreement remains in effect; or

(ii) Prove or Vendor as applicable retains any Personal Data related to the Master Agreement in its possession or control (the "**Term**").

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Data shall remain in full force and effect.

10.3 Any party's failure to comply with the terms of this DPA is a material breach of the Master Agreement. In such event, non-breaching party may terminate the Master Agreement effective immediately upon written notice to the counterparty without further liability or obligation.

10.4 If a change in applicable Privacy and Data Protection Laws prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements, unless the parties otherwise agree on an alternate remediation plan. If the parties are unable to bring the Personal Data processing into compliance with the Privacy and Data Protection Laws within thirty (30) days, either party may terminate the Master Agreement upon written notice to the other party.

11. DATA RETURN AND DESTRUCTION

11.1 At Prove's request, Vendor shall promptly destroy or return to Prove all copies of, or access to, the Prove Personal Data in its possession or control, in the format and on the media reasonably specified.

11.2 On termination of the Master Agreement for any reason or expiry of its term, each party will promptly (and no later than 30 days) return or destroy all Confidential Information belonging to the other party unless retention of such data is necessary for reasonable archival, billing, legal, and regulatory compliance purposes. For the avoidance of doubt, retained Confidential Information shall not be used for any other purpose than for archival, billing, legal, and regulatory compliance.

11.3 If retention is necessary for archival, billing, legal, or regulatory compliance purposes as set out in Section 11.2 above, Vendor shall notify Prove in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.4 At Prove's request, Vendor shall certify in writing that it has destroyed all Prove Personal Data as requested in Section 11.1 or 11.2.

12. RECORDS

12.1 Vendor shall keep detailed, accurate, and up-to-date records regarding any processing of Personal Data it carries out on behalf of the controller, including but not limited to, the access, control, and security of the Personal Data, approved subcontractors and affiliates, and the processing purposes ("**Records of Processing**"). The parties, when acting as controllers, shall also maintain adequate Records of Processing incompliance with applicable Data Protection & Privacy Laws.

12.2 The party acting as processor shall ensure that the Records of Processing are sufficient to enable the controller to verify the processor's compliance with its obligations under this DPA.

13. AUDIT & ASSURANCE

13.1 Each party shall periodically audit its Personal Data processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this DPA.

13.2 Each party agrees to allow the other party to assess and verify compliance with this DPA on a regular basis, but no more once than annually, for at least the length of the engagement ("**Annual Reviews**"). This may include, as determined by the other party, access to or copies of documentation related to the Information Security Program, including but not limited to the information security policies and procedures, as well as any recent external, third party assurance documentation (e.g., SOC 2, Type II report, PCI DSS 3.2 attestation of compliance, ISO 27001 certification, etc.), and the results of any security testing, including summary reports, test details and dates, and information on remediation related to any findings.

14. WARRANTIES

14.1 The party acting as controller warrants and represents that it has:

(i) obtained all required consent(s) under applicable Privacy and Data Protection Laws to process Services Personal Data in order to receive the Services; and

(ii) provided all required privacy notice(s) under applicable Privacy and Data Protection Laws to process Services Personal Data in order to receive the Services.

14.2 Each party warrants and represents that:

(i) its employees, subcontractors, agents, and any other person or persons accessing Personal Data on its behalf are reliable and trustworthy and have received the required training on the Privacy and Data Protection Laws relating to the Personal Data;

(ii) it and anyone operating on its behalf will process the Personal Data in compliance with all applicable Privacy and Data Protection Laws and other laws, enactments, regulations, orders, standards, and other similar instruments;

(iii) it has no reason to believe that any Privacy and Data Protection Laws prevent it from providing any of the Services under the Master Agreement; and

(iv) considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Data and the accidental loss or destruction of, or damage to, Personal Data, and ensure a level of security appropriate to:

(a) the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction, or damage;

(b) the nature of the Personal Data protected; and

(c) comply with all applicable Privacy and Data Protection Laws, as well as its information and security policies, including the security requirements required in Section 5.

14.3 Each party warrants and represents that its expected use of any Personal Data as part of the Services complies with this DPA and all Privacy and Data Protection Laws.

15. NOTICE

15.1 Any notice or other communication given to a party under or in connection with this DPA shall be in writing by email, certified mail, hand delivery, or delivery by a reputable next business day carrier service delivered to:

For Prove:

Prove Identity, Inc.
245 Fifth Avenue, 20th Floor
New York, NY 10016
Attn: Chief Compliance Officer
compliance@prove.com

15.2 Section 14.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16. CONFIDENTIALITY

16.1 Each party shall treat Personal Data as Confidential Information. Each party shall ensure that its personnel and Sub-processors are subject to confidentiality obligations as least as restrictive as in the Master Agreement and this DPA.

16.2 Such confidentiality obligations shall survive the termination of this engagement.

17. MISCELLANEOUS

17.1 Neither party shall assign or transfer any rights or delegate any duties hereunder, in whole or in part, by operation of law or otherwise, without the other party's express prior written consent, which will not be unreasonably withheld or delayed.

17.2 The terms of this DPA shall control to the extent there is any conflict between this DPA and the terms of the Master Agreement. Except as specifically amended and modified in writing by the parties, the terms and provisions of this DPA shall remain in full force and effect.

17.3 Without limiting the foregoing, the governing law clause and forum selection clause of the Master Agreement shall apply to any disputes arising out of this DPA.