DATA PROCESSING ADDENDUM

1. BACKGROUND

1.1 In accordance with clause 3.4 of the Agreement, this Data Processing Addendum ("**DPA**") sets out the basis on which PROOF processes Customer Personal Data (as defined below).

1.2 In the event of a conflict between any of the provisions of this DPA and the remaining provisions of the Agreement, the provisions of this DPA shall prevail.

2. DEFINITONS

2.1 Unless otherwise set out below, each capitalised term in this DPA shall have the meaning set out in the Agreement and the following capitalised terms used in this DPA shall be defined as follows:

(a) "**Customer Personal Data**" means the personal data described in ANNEX 1 and any other personal data that PROOF processes on behalf of the Customer in connection with PROOF's provision of the Service;

(b) "**Data Protection Laws**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**") and all applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the Processing of Customer Personal Data;

(c) "**European Economic Area**" or "**EEA**" means the Member States of the European Union together with Iceland, Norway, and Liechtenstein;

(d) "**Security Incident**" means any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Customer Personal Data;

(e) "**Standard Contractual Clauses**" means the Standard Contractual Clauses (processors) approved by European Commission Decision C(2010)593 or any subsequent version thereof released by the European Commission (which will automatically apply);

(f) "**Subprocessor**" means any Processor engaged by PROOF who agrees to receive from PROOF Customer Personal Data; and

(g) the terms "**personal data**", "**Controller**", "**Processor**", "**Data Subject**", "**Process**" and "**Supervisory Authority**" shall have the same meaning as set out in the GDPR.

3. DATA PROCESSING

3.1 **Instructions for Data Processing.** PROOF will only Process Customer Personal Data in accordance with (a) the Agreement, to the extent necessary to provide the Service to the Customer, and (b) the Customer's written instructions, unless Processing is required by

European Union or Member State law to which PROOF is subject, in which case PROOF shall, to the extent permitted by applicable law, inform the Customer of that legal requirement before Processing that Customer Personal Data.

3.2   Processing outside the scope of this Agreement will require prior written agreement between the Customer and PROOF on additional instructions for Processing.

3.3   **Required consents.** Where required by applicable Data Protection Laws, the Customer will ensure that it has obtained/will obtain all necessary consents for the Processing of Customer Personal Data by PROOF in accordance with the Agreement.

3.4   **Privacy Shield**. PROOF is currently in the process of preparing to self-certify its compliance under Privacy Shield. PROOF intends to self-certify under Privacy Shield at the soonest practicable opportunity. Although it has not yet self-certified under Privacy Shield, PROOF agrees to conduct its activities in accordance with the requirements of the Privacy Shield Principles. To the extent that PROOF processes any Customer Personal Data protected by Data Protection Laws under the Agreement and/or that originates from the EEA, to the United States, the parties acknowledge that PROOF shall be deemed to provide adequate protection (within the meaning of Data Protection Laws) for any such Customer Personal Data as though it has self-certified its compliance with Privacy Shield. PROOF agrees to protect such Customer Personal Data in accordance with the requirements of the Privacy Shield Principles. If PROOF is unable to comply with this requirement, PROOF shall inform Customer.

4.   SUBPROCESSORS

4.1   **Consent to Subprocessor Engagement**. The Customer generally authorises the engagement of third parties as Subprocessors.

4.2   **Information about Subprocessors**. A list of PROOF's Subprocessors is available at http://proof-legal-public.s3-website-us-east-1.amazonaws.com/PROOF_Subprocessors.pdf and may be updated by PROOF from time to time in accordance with this DPA.

4.3   **Requirements for Subprocessor Engagement**. When engaging any Subprocessor, PROOF will:

(a)   ensure via a written agreement that:

(i)   the Subprocessor only accesses and uses Customer Personal Data to the extent required to perform the obligations subcontracted to it and does so in accordance with the Agreement and this DPA; and

(ii)   the same obligations are imposed on the Subprocessor with regard to their Processing of Customer Personal Data, as are imposed on PROOF under this DPA.

(b) remain full liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

4.4 **Opportunity to Object to Subprocessor Changes.**

(a) When any new Subprocessor is engaged during the Agreement, PROOF will inform Customer of the engagement.

(b) Customer may object to the appointment of that Subprocessor by providing documentary evidence that reasonably shows that the Subprocessor does not or cannot comply with the requirements in this DPA ("**Objection**"). If PROOF does not remedy or provide a reasonable workaround for your Objection within a reasonable time, Customer may object to any new Subprocessor by terminating the Agreement immediately upon written notice to HQ Mobile, on condition that Customer provides such notice within 90 days of being informed of the engagement of the subprocessor as described in clause 4.4(a). This termination right is Customer's sole and exclusive remedy if Customer objects to any new Subprocessor.

4.5 **Transfers of Personal Data Outside the EEA.** To the extent that the Processing of Customer Personal Data by PROOF involves the export of such Personal Data to a country or territory outside the EEA, such transfer shall be to a third party:

   a) in a country subject to an adequacy decision by the European Commission;

   b) that is a member of a compliance scheme recognised by the European Commission as offering adequate protection for the rights and freedoms of data subjects such as the EU-U.S. Privacy Shield; or

   c) that has signed Standard Contractual Clauses (processors) approved by European Commission Decision C(2010)593 or any subsequent version thereof released by the European Commission, (with the Customer as data exporter and the third party as data importer). For this purpose, the Customer appoints PROOF to act as its agent with the authority to complete and enter into the Standard Contractual Clauses as agent for the Customer on its behalf for this purpose.

5. **DATA SECURITY, AUDITS AND SECURITY NOTIFICATIONS**

5.1 **PROOF Security Obligations**. Taking into account 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, PROOF shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including, where applicable by virtue of Article 28(3)(c) of the GDPR, and as appropriate, the measures referred to in Article 32(1) of the GDPR. Without limiting the generality of the foregoing, PROOF shall put in place and maintain the technical and organisational measures set out in ANNEX 2.

5.2 **Security Audits**. The Customer may, upon reasonable notice, audit (by itself or using independent third party auditors) PROOF's compliance with the security measures set out

in this DPA (including the technical and organisational measures as set out in ANNEX 2), including by conducting audits of PROOF's (and Suprocessors') data processing facilities. Upon request by the Customer, PROOF shall make available all information reasonably necessary to demonstrate compliance with this DPA.

5.3 **Security Incident Notification.** If PROOF or any Subprocessor becomes aware of a Security Incident, PROOF will (a) notify the Customer of the Security Incident within 72 hours, (b) investigate the Security Incident and provide such reasonable assistance to the Customer (and any law enforcement or regulatory official) as required to investigate the Security Incident, and (c) take steps to remedy any non-compliance with this DPA.

5.4 **PROOF Employees and Personnel.** PROOF shall treat the Customer Personal Data as the Confidential Information of the Customer, and shall ensure that:

(a) access to Customer Personal Data is limited to those employees or other personnel who have a business need to have access to such Customer Personal Data;

(b) any employees or other personnel have agreed in writing to protect the confidentiality and security of Customer Personal Data.

6. ACCESS REQUESTS AND DATA SUBJECT RIGHTS

6.1 **Data Subject Requests**. Save as required (or where prohibited) under applicable law, PROOF shall notify the Customer of any request received by PROOF or any Subprocessor from a Data Subject in respect of their personal data included in the Customer Personal Data, and shall not respond to the Data Subject.

6.2 PROOF shall, where possible, assist the Customer with ensuring its compliance under applicable Data Protection Laws, and in particular shall:

(a) provide the Customer with the ability to correct, delete, block, access or copy the personal data of a Data Subject, or

(b) promptly correct, delete, block, access or copy Customer Personal Data within the Services at the Customer's request.

6.3 **Government Disclosure.** PROOF shall notify the Customer of any request for the disclosure of Customer Personal Data by a governmental or regulatory body or law enforcement authority (including any data protection supervisory authority) unless otherwise prohibited by law or a legally binding order of such body or agency.

6.4 **Data Subject Rights.** Where applicable, and taking into account the nature of the Processing, PROOF shall use all reasonable endeavours to assist the Customer by implementing any other appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising Data Subject rights laid down in the GDPR.

7. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

7.1 To the extent required under applicable Data Protection Laws, PROOF shall provide reasonable assistance to the Customer with any data protection impact assessments and with any prior consultations to any Supervisory Authority of the Customer, in each case solely in relation to Processing of Customer Personal Data and taking into account the nature of the Processing and information available to PROOF.

8. DURATION AND TERMINATION

8.1 **Deletion of data**. Subject to 8.2 and 8.3 below, PROOF shall, within 90 (ninety) days of the date of termination of the Agreement:

    (a) return a complete copy of all Customer Personal Data by secure file transfer in such a format as notified by the Customer to PROOF; and

    (b) delete and use all reasonable efforts to procure the deletion of all other copies of Customer Personal Data Processed by PROOF or any Subprocessors.

8.2 Subject to section 8.3 below, the Customer may in its absolute discretion notify PROOF in writing within 30 (thirty) days of the date of termination of the Agreement to require PROOF to delete and procure the deletion of all copies of Customer Personal Data Processed by PROOF. PROOF shall, within 90 (ninety) days of the date of termination of the Agreement:

    (a) comply with any such written request; and

    (b) use all reasonable endeavours to procure that its Subprocessors delete all Customer Personal Data Processed by such Subprocessors,

and, where this section 8.2 applies, PROOF shall not be required to provide a copy of the Customer Personal Data to the Customer.

8.3 PROOF and its Subprocessors may retain Customer Personal Data to the extent required by applicable laws and only to the extent and for such period as required by applicable laws and always provided that PROOF shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable laws requiring its storage and for no other purpose.

ANNEX 1

DETAILS OF THE PROCESSING OF CUSTOMER PERSONAL DATA

This ANNEX 1 includes certain details of the processing of Customer Personal Data as required by Article 28(3) of the GDPR.

Subject matter and duration of the Processing of Customer Personal Data

- The subject matter and the duration of the Processing of the Customer Personal Data are set out in the Agreement including this DPA.

The nature and purpose of the Processing of Customer Personal Data

- The Customer Personal Data will be subject to the following basic Processing activities: transmitting, collecting, storing, and analysing data in order to provide the Service to the Customer, and any other activities related to the provision of the Service or as specified in the Agreement.

The types of Customer Personal Data to be Processed

- Contact information, such as first name, last name, and email address.
- Device information, such as browser type and version, IP address, operating system and version.
- Activity and usage information, such as page visits, clicks and other actions taken on Customer sites and services.
- Any other Customer Personal Data provided by the Customer in connection with the Service.

The categories of Data Subject to whom the Customer Personal Data relates

- The categories of Data Subject to whom the Customer Personal Data relates concern are set out in the Agreement including this DPA

The obligations and rights of the Customer

- The obligations and rights of the Customer are as set out in the Agreement including this DPA

ANNEX 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1.   PROOF maintains internal policies and procedures, or procures that its Subprocessors do so, which are designed to:

   (a)   secure any personal data Processed by PROOF against accidental or unlawful loss, access or disclosure;

   (b)   identify reasonably foreseeable and internal risks to security and unauthorised access to the personal data Processed by PROOF;

   (c)   minimise security risks, including through risk assessment and regular testing.

2.   PROOF will, and will use reasonable efforts to procure that its Subprocessors conduct periodic reviews of the security of their network and the adequacy of their information security program as measured against industry security standards and its policies and procedures.

3.   PROOF will, and will use reasonable efforts to procure that its Subprocessors periodically evaluate the security of their network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.