First Advantage

BACKGROUND SCREENING SERVICES AND DATA PROCESSING ADDENDUM
European Economic Area (EEA) & United Kingdom

This Background Screening Service Addendum – European Economic Area and United Kingdom ("Addendum") is made and entered into by and between First Advantage Europe Ltd. ("Service Provider"), and _____ ("Client"), on behalf of itself and on behalf of its Authorised Affiliates (defined below), pursuant to the Master Services Agreement entered into on the ____ day of _____ 20____ ("MSA").

1. **DESCRIPTION OF SERVICES.** Client may order the Services set forth in Schedule A in the EEA and United Kingdom ("UK") from Service Provider, having its principal place of business at 2 St. Johns Street, Colchester CO2 7AA, United Kingdom, in accordance with their respective rights and obligations under the General Data Protection Regulation ("GDPR") and the Data Protection Laws as defined below and pursuant to the terms and condition of this Addendum. Client shall pay Service Provider for all Services as outlined in Schedule A.

2. **DEFINITIONS AND INTERPRETATION.**

2.1 Capitalised terms used but not defined in this Addendum have the meaning given to them in the MSA or in any referenced terms and conditions herein. Reference to any statute or statutory provision shall include a reference to any statute or statutory provision which amends, extends, consolidates or replaces the same (save to the extent that any amendment, extension, consolidation or replacement would impose more onerous obligations than otherwise exist at the date of this Addendum) or which has been amended, extended, consolidated or replaced by the same and shall include any orders, regulations, instruments or other subordinate legislation made under the relevant statute or statutory provision.

2.2 The singular includes the plural and vice versa and any gender includes all genders.

2.3 The following are defined terms:

Authorised Affiliate means any of Client's affiliate(s) which (a) is subject to the Data Protection Laws and (b) is permitted to use the Services pursuant to the MSA between Client and Service Provider, but has not signed an agreement directly with Service Provider and is not a "Client" or "Customer" as defined under the MSA;

Authorised Third Party means any party that provides certain services to the Client and is authorized to access Service Provider's delivery platform for the purpose of obtaining Personal Data on behalf of the Client as set forth herein;

Data Controller means the entity which determines the purposes and means of the Processing of Personal Data;

Data Processor means the entity which Processes Personal Data on behalf of the Data Controller;

Data Protection Laws means (a) the GDPR; (b) the UK GDPR and UK Data Protection Act 2018 (c) the FADP and (d) all other applicable laws under the jurisdiction of the EEA member states and in UK or Switzerland concerning the Processing of data relating to living persons under the MSA;

Data Subject means each identified or identifiable (whether directly or indirectly) natural person to whom any Personal Data relates;

EEA means the European Economic Area;

EEA Personal Data means the processing of Personal Data to which data protection legislation of the European Union, or of a Member State of the European Union or European Economic Area was applicable prior to its processing by Service Provider;

FADP means the Swiss Federal Act on Data Protection;

GDPR means Regulation (EU) 2016/679 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

Personal Data means information relating to an identified or identifiable living individual whose data was Processed as part of the Services performed by Service Provider for Client;

Personal Data Breach means any actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed, while under the control of Service Provider;

Processing means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Protected Area means:

a. in the case of EEA Personal Data, the members states of the European Union and the Economic Area and any country, territory, sector or international organisation in respect of which an adequacy decision under Art.45 GDPR is in force;
b. in the case of UK Personal Data, the United Kingdom and any country, territory, sector or international organisation in respect of which an adequacy decision under United Kingdom data protection legislation or United Kingdom adequacy regulations is in force; and

c. in the case of Swiss Personal Data, any country, territory, sector or international organisation which is recognised as adequate under the laws of Switzerland;

Relevant Law means:

a. in the case of EEA Personal Data, any legislation of the European Union, or of a Member State of the European Union or European Economic Area;
b. in the case of UK Personal Data, any legislation of any part of the United Kingdom; and
c. in the case of Swiss Personal Data, any legislation of Switzerland;

Services means those services performed by Service Provider for Client under the MSA;

Standard Contractual Clauses means:

d. in respect of EEA Personal Data, the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR, adopted by the European Commission under Commission Implementing Decision (EU) 2021/914 ("EU Standard Contractual Clauses"); and
e. in respect of Swiss Personal Data, the EU Standard Contractual Clauses, provided that any references in the clauses to the GDPR shall refer to the FADP, the term 'member state' must not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence in accordance with clause 18(c) of the clauses and the clauses shall also protect the data of legal persons until the entry into force of the revised FADP; and
f. in respect of UK Personal Data, the International Data Transfer Addendum to the EU Standard Contractual Clauses, issued by the Information Commissioner and laid before Parliament in accordance with s.119A of the Data Protection Act 2018 on 2 February 2022 ("UK Standard Contractual Clauses");

Swiss Personal Data means Personal Data to which the FADP was applicable prior to its processing by Service Provider;

UK GDPR means the GDPR as applicable as part of UK domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended); and

UK Personal Data means Personal Data to which the UK GDPR and UK Data Protection Act 2018 were applicable prior to its processing by Service Provider.

3. GENERAL TERMS.

3.1 **General GDPR Terms.**

a. To the extent that Service Provider Processes Personal Data in the course of providing the Services, each party acknowledges that, for the purpose of Data Protection Laws, Client, or its Authorised Affiliate, is the Data Controller of the Personal Data and Service Provider is the Data Processor. In this Addendum, reference to Client shall also include Authorised Affiliates unless specifically excluded, provided that Client has previously identified the Authorised Affiliates that seek to rely on this Addendum to Service Provider. Any obligation on Service Provider to notify or forward information to Client under this Addendum shall be met by a notice to Client alone, and Client shall be responsible for relaying any information or notice to its Authorised Affiliates.

b. Service Provider shall implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of the Data Protection Laws and ensure the protection of the rights of the Data Subject.

c. Processing by Service Provider shall be governed by this Addendum and the MSA under any Data Protection Laws, which is binding on Service Provider with regard to Client. The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of personal data, the categories of data subjects and the obligations and rights of Client are set forth in Appendix 1 (as amended by the parties from time to time).

d. Service Provider shall:

(i) only Process that Personal Data in accordance with the documented instructions of Client (including to the extent necessary to provide the Services and to comply with its obligations under the MSA and this Addendum) unless Processing is required by Relevant Law to which Service Provider is subject, in which case Service Provider will to the extent permitted by Relevant Law inform Client of that legal requirement before Processing such Personal Information;

(ii) inform Client if, in Service Provider's opinion, any of Client's instructions would breach Data Protection Laws; and

(iii) reasonably assist the Client with implementing privacy by design and default and/or its equivalent under Data Protection Laws taking account the state of the art, the costs of implementation and the nature, scope, context and purpose of Processing. The Service Provider shall comply with applicable data protection initiatives such as privacy by design and default if and to the extent it is required to be complied under the Data Protection Laws;

(iv) assist Client with undertaking an assessment of the impact of Processing that Personal Data, and with any consultations with a supervisory authority, if and to the extent an assessment or consultation is required to be carried out under Data Protection Laws in each case solely in relation to processing of Personal Data by, and taking account the nature of the Processing and the information available to Service Provider.

3.2 **Data Subject Rights.** Service Provider shall:

a. implement appropriate technical and organisational measures for the fulfilment of Client's obligation to respond to requests by Data Subjects to exercise their rights of access, rectification or erasure, to restrict or object to Processing of Personal Data, or to data portability; and

b. if a Data Subject makes a written request to Service Provider to exercise any of the rights referred to in Section 3.2(a), forward the request to Client promptly and shall, upon Client's reasonable written request, provide Client with all co-operation and assistance reasonably requested by Client in relation to that request to enable Client to respond to that request in compliance with applicable deadlines and information requirements.

3.3 **Authorised Third Party.** If Client uses an Authorised Third Party, who will have access to the Services and/or Personal Data, Client shall ensure that this Authorised Third Party shall comply with the terms and conditions of (i) the MSA, (ii) any Local Country Agreement, (iii) this Addendum and (iv) the terms and conditions as set forth in Appendix 3.

3.4 **Security.** Service Provider shall:

a. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purpose of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement and maintain appropriate technical and organisational measures as set forth in Appendix 2 to ensure a level of security appropriate to the risk, including the risk of unauthorised or unlawful Processing of Personal Data, and of accidental or unlawful loss, alteration, unauthorised disclosure or destruction of, or damage to, Personal Data;

b. notify Client without undue delay after becoming aware of a Personal Data Breach, and upon Client's reasonable written request, provide Client with all cooperation and assistance reasonably requested by Client to enable Client to notify the Personal Data Breach to the relevant supervisory authority and relevant Data Subject(s) (as applicable); and

c. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.5 **Sub-Processing of Personal Data.** Service Provider shall:

a. not engage another processor without prior specific or general written authorisation of Client. Client authorises Service Provider to use the sub-processors listed at the time this Addendum is signed, and to appoint new sub-processors or replace existing sub-processors provided that Service Provider notifies Client at least 3 working days in advance of its intended changes by updating the list above-mentioned, and received no business objection from the Client in this period. If the Client objects to the change of a relevant sub-processor used for the Services provided to the Client within such period on the basis of legitimate data protection concerns, Service Provider shall use all reasonable efforts to make available a change in the associated Processing services to avoid the Processing of Personal Data by the objected-to sub-processor. If Service Provider is unable to make this change within a reasonable time period, or Client does not approve such change, Client may, by providing written notice to Service Provider, terminate the associated Processing service which cannot be provided without the use of the objected-to sub-processor;

b. before disclosing Personal Data to any processor, enter into a contract with that processor under which the processor agrees to comply with privacy obligations at least as protective as those required by this Addendum, or with obligations at least as protective as those implemented by Service Provider to protect its own personal data of a similar nature. Where that other processor fails to fulfil its data protection obligations, the Service Provider shall remain fully liable to the Client for the performance of that other processor's obligations.

3.6 **Transfers of Personal Data.**

a. Service Provider shall not transfer Personal Data outside of the applicable Protected Area unless where Service Provider proposes to transfer EEA Personal Data, UK Personal Data or Swiss Personal Data to a processor outside of the applicable Protected Area as permitted under section 3.5, Service Provider enters into the appropriate module (being module 3) of the appropriate Standard Contractual Clauses under Relevant Law with such processor. In complying with its obligations under Article 3.5(b) to put in place obligations at least as protective as those required by this Addendum in its contract with a processor, the parties agree that in the event of any conflict between a section of this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail;

b. Where any mechanism for cross-border transfers of Personal Data on which the parties have relied is found by a supervisory authority, court of competent jurisdiction or other governmental authority to be an invalid means of complying with the restrictions on transferring Personal Data to a third country or territory as set out in Data Protection Laws, the parties shall act in good faith to agree the implementation of an alternative solution to enable Client and/or Service Provider to comply with the provisions of Data Protection Laws in respect of any such transfer.

3.7 **Assistance and Review.** Service Provider shall:

a. promptly notify Client if it receives any complaint, notice or communication which relates directly or indirectly to the Processing of Personal Data, or to either party's compliance with Data Protection Laws, and shall fully co-operate and assist Client in relation to any such complaint, notice, communication or non-compliance; and

b. upon Client's reasonable written request, Service Provider will allow Client to audit or obtain reasonably reliable documentation regarding the adequacy of the data processing facilities used by the Service Provider to Process Personal Data on behalf of the Client. Such audit or documentation may: (i) be an annual SOC2 (or subsequent successor) audit of the Service Provider's security policies and procedures; (ii) be in accordance with ISO 27001 standards or such alternative standards that are substantially equivalent to ISO 27001; or (iii) otherwise provide for demonstrable assurances of adequacy of the data processing facilities used by the Service Provider to Process Personal Data on behalf of the Client ("Audit

Report"). If the Client requests in writing, Service Provider will provide the Client with a copy of the Audit Report or related documentation so that the Client can reasonably verify the Service Provider's compliance with the security obligations under Data Protection Laws.

c. Information and audit rights of Client only arise under section 3.7 to the extent that the MSA does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

d. Service Provider has appointed a data protection officer in accordance with the GDPR. Such individual may be reached at GDPR@FADV.com.

3.8 **Termination or Expiry.** Service Provider shall, unless expressly stated otherwise in this Addendum or the MSA, upon termination or expiry of the MSA, Service Provider shall, and shall ensure that each processor shall, immediately cease to use the Personal Data; Service Provider shall, at Client's option and request, return the Personal Data to Client, or delete the Personal Data and all copies and extracts of the Personal Data unless required to retain a copy in accordance with Relevant Law.

4. ADDITIONAL TERMS.

4.1 **UNITED KINGDOM CRIMINAL Disclosure checks.** The parties acknowledge and agree that to the extent Client orders UK disclosure check services from Service Provider, the terms and conditions located at http://images.learn.fadv.com/Web/FirstAdvantageCorporation/{1da205a4-05d3-4a26-95eb-5a48aebb4860}_UK_Disclosure_Checks_Terms.pdf shall apply.

4.2 **DIGITAL ID.** The parties acknowledge and agree that to the extent Client orders Digital ID services from Service Provider, the terms and conditions located at https://fadv.com/wp-content/uploads/DigitalID_Terms.pdf shall apply.

4.3 **DRIVER AND VEHICLE LICENSING AGENCY.** The parties acknowledge and agree that to the extent Client orders Driver and Vehicle Licensing Agency check services from Service Provider, the terms and conditions located at https://fadv.com/dvla-terms-2/ shall apply.

4.4 **EXPERIAN.** The parties acknowledge and agree that to the extent Client orders Experian services from Service Provider, the terms and conditions located at https://fadv.com/wp-content/uploads/Experian_Flow_Down_Terms.pdf shall apply.

4.5 **ID3GLOBAL AND PAF SOLUTION.** The parties acknowledge and agree that to the extent Client orders ID3Global and PAF Solution services from Service Provider, the terms and conditions located at https://fadv.com/id3-terms/ shall apply.

5. MISCELLANEOUS PROVISIONS.

5.1 This Addendum may be executed in any number of counterparts, all of which, taken together, shall constitute one and the same agreement, and any party (including any duly authorised representative of a party) may enter into this Addendum by executing a counterpart.

5.2 If there is any conflict or inconsistency between this Addendum and the other terms of the MSA, this Addendum will govern. Except for changes made by this Addendum, the MSA remains unchanged and in full force and effect and the original effective date (or equivalent) as defined in the MSA shall remain the same.

5.3 Client agrees it is the end-user of all reports, and will not resell, sub-license, deliver, display, or otherwise distribute any report, or provide any information in any report, to any third party, except as otherwise required or permitted under applicable law.

5.4 Client agrees not to market the reports through the Internet.

5.5 Service Provider may impose additional requirements in connection with Client orders and use of reports in order to comply with changes in laws, to better protect the security and privacy of the information Service Provider provide or as Service Provider otherwise reasonably believes to be prudent or as required under the circumstances. Client agrees to comply with all such additional requirements after Client has received notice of them.

5.6 This Addendum and any non-contractual obligations arising out of or in connection with it are governed by English law.

This Addendum is signed by the duly authorised representatives of the parties as of the Effective Date.

Client:		Service Provider:	**First Advantage Europe Ltd.**
By:		By:	
Name:		Name:	Bret T. Jardine
Title:		Title:	EVP, General Counsel
Date:		Date:	

APPENDIX 1

Details of Service Provider	
Details of DPO	HewardMills, 77 Farringdon Road, London EC1M 3JU
DPO Contact Details	gdpr@fadv.com
Description of Processing	
Duration of Processing	The term of any existing agreement between Client and Service Provider relating to the services covered herein.
Nature of Processing	Facilitating and Processing background screening services
Purpose of Processing	Employment screening services performing data Processing activities
Frequency of data transfers	Transfers limited to the extent necessary to provide the Services under the MSA between Client and Service Provider
Client Personal Data	
Data subjects	Current and prospective employees and/or contractors of Client
Data categories (to be updated as necessary)	Name; maiden name; alias(es); current and previous addresses; birth date; birth place; ID number (which may include passport, national ID card, driver's license); mother/father's complete name; employer name; employer contact details; manager name; manager contact details; job title; pay rate; dates of employment; reason for leaving employment; school name; school contact details; student number; qualification details; field of study; school attendance dates; school graduation dates.
Sensitive Personal Data	Criminal records if criminal checks ordered by Client
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period	2 years unless the Client requires a shorter or a longer period.
Transfers to processors	
Subject matter, nature and duration of the processing	Transfers limited to the extent necessary to provide the Services under the MSA between Client and Service Provider
Competent Supervisory Authority	The Belgium Data Protection Authority in respect of EEA Personal Data; the ICO in respect of UK Personal Data; the Federal Data Protection and Information Commissioner in respect of Swiss Personal Data.

APPENDIX 2

The Service Provider maintains and enforces technical and organizational security measures to protect personal data and systems. The following sections describe some of the primary controls implemented by the Service Provider:

1. Information Security Policies and Standards

The Service Provider will implement security requirements users who have access to personal data. These are designed to:

- Prevent unauthorized persons from gaining access to personal data processing systems (physical access control);
- Prevent personal data processing systems from being used without appropriate authorization (logical access control);
- Ensure that persons entitled to use a personal data processing system gain access to only such personal data as they are entitled to access in accordance with their access rights and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorization (data access control);
- Ensure that personal data cannot be read, copied, modified or deleted without authorization during electronic transmission over public networks, physical transport or storage, and that the target entities for any transfer of personal data by means of data transmission facilities can be established and verified (data transfer control);
- Ensure the establishment of an audit trail to document whether and by whom personal data have been entered into, modified in, or removed from personal data processing (entry control);
- Ensure that personal data are processed solely in accordance with the instructions (control of instructions);
- Ensure that personal data and protected against accidental destruction or loss (availability control);

2. Physical Security

- Service Provider shall maintain a physical security program to include the following controls:
- Service Provider shall formally document a corporate physical security policy. This policy is communicated to employees and updated regularly to govern access to these data centers. The corporate physical security policy requires minimum physical security implementations for all sites.
- Visitors are required to sign in at the front desk and issued a visitor's badge and are escorted at all times by a guard or Service Provider authorized employee. Control logs are recorded and retained and are reviewed regularly.
- Alarm sensors are installed on external doors to facilities.
- Badge access system secures access into facilities.

3. Personnel Security

The Service Provider shall implement a security awareness program to train personnel about their security obligations and Service Provider security policies and processes. This program includes training about data classification and handling responsibilities, physical security, security policies and practices, and reporting of security incidents.

4. Access Control

Service Provider shall maintain access control procedures and requirements:

- Service Provider system users have the least privilege required to perform job duties
- Only authorized administrators can grant, modify or revoke access to an information system that processes or stores personal data
- All Service Provider's systems require unique identifiers for each user.
- Passwords must meet strict complexity rules, including minimum length, special characters, etc.
- Passwords must be changed periodically.

5. Network Security

The Service Provider shall implement and maintain network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and or/or prevention systems, access control lists and routing protocols.

6. Data Security

The Service Provider maintains a data classification and protection program. Personal data and other sensitive information is classified, labelled and handled as Confidential Data. Industry standard encryption protects confidential data across the public network. Data is encrypted while at rest when it is stored. Removable media and portable computers are encrypted when used to store personal data.

7. Virus and Malware Controls

The Service Provider shall maintain anti-virus and malware protection on Service Provider systems.

8. Incident Management

The Service Provider shall maintain a security incident response program to manage security incidents throughout their lifecycle.

9. Business Continuity and Disaster Recovery

The Service Provider shall implement and maintain appropriate business continuity and disaster recovery plans and processes.

Terms and Conditions for Authorised Third Party

1. **User Restrictions.** Client agrees and undertakes that the Authorised Third Party:

   a. shall use the Personal Data solely for the purposes permitted in the MSA and any Addendum and for no other purpose, including, without limitation, statistical analysis.

   b. shall keep all Personal Data strictly confidential except as required by law.

   c. shall interface with Service Provider only for the purpose of ordering and receiving Personal Data for Client from Service Provider and for no other purpose.

   d. has no right of access to Service Provider products or services independent of Client.

   e. shall provide Personal Data to Client unchanged and to Client only, and Authorised Third Party / shall be responsible for authenticating the end-user Client of the reports or Personal Data and for ensuring that Client is only accessing Personal Data via a discrete customer account identification number in accordance with technical requirements provided to Authorised Third Party by Service Provider.

   f. shall not resell Personal Data to anyone, whether another customer of Service Provider or of Authorised Third Party, or otherwise, either alone or in combination with information from other data sources.

   g. shall not transfer or otherwise disseminate Personal Data to anyone other than Client, either alone or in combination with other data services. No Personal Data shall be stored by Authorised Third Party / in any database except that information provided for the use of Client may remain available for later use by Client.

   h. shall implement the appropriate technical and organizational measures as set forth in Article 32 of the GDPR.

   i. shall maintain for a period of three years a complete and accurate record, including the identity of the individual ordering the report with regard to every access to Personal Data obtained from Service Provider.

   j. will not make any public announcement concerning this Agreement unless and until the other party has approved such announcement. The parties and the Authorised Third Party agree that they will not distribute or use marketing pieces or brochures utilizing the trade names/trademarks of the other party without express written approval from the owner of the trade name/trademark.

2. **Confidentiality.** Client agrees and undertakes that Authorised Third Party shall adhere to confidentiality provisions no less restrictive than the provisions of confidentiality terms as set forth in the MSA.

3. **Security Event.** Client agrees and undertakes that Authorised Third Party shall acknowledge that, upon unauthorized acquisition or access of or to Personal Data while in Authorised Third Party's possession or under its control, including but not limited to that which is due to use by an unauthorized person or due to unauthorized use (a "Security Event"), Authorised Third Party shall, in compliance with applicable Data Protection Laws, notify the Data Controller that a Security Event has occurred, and shall also notify the Service Provider. Client agrees and undertakes that Authorised Third Party shall agree that such notification shall not reference Service Provider or the product through which the Personal Data was provided, nor shall Service Provider be otherwise identified or referenced in connection with the Security Event, without Service Provider's express written consent. Client shall be solely responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Security Event and shall bear all costs associated with complying with legal and regulatory obligations in connection therewith. Client agrees and undertakes that Authorised Third Party shall remain solely liable for claims that may arise from a Security Event, including, but not limited to, costs for litigation (including attorneys' fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Security Event, and to the extent that any claims are brought against Service Provider, shall indemnify Service Provider from such claims. In the event of a Security Event, Service Provider may, in its sole discretion, take immediate action, including suspension or termination of Authorised Third Party's account, without further obligation or liability of any kind.

4. **Audit Rights.** Client agrees and undertakes that Service Provider shall have the right to conduct periodic audits of Authorised Third Party's use of the Services ordered pursuant to the MSA and the Addendum. In addition, certain third party suppliers or Data Protection Authorities may require the right to audit Authorised Third Party either directly or through Service Provider. The scope and frequency of any audit shall be at the reasonable discretion of Service Provider but will be subject to requirements imposed by third party suppliers. Service Provider will provide reasonable notice prior to conducting any audit provided that Service Provider has received reasonable notice from any third party supplier involved in the audit process. Any violations discovered as a result of such audit may be cause for immediate action by Service Provider, including, but not limited to, immediate termination of the MSA and any applicable Addendum.

5. **DISCLAIMER OF WARRANTIES.** CLIENT MUST NOTIFY AUTHORISED THIRD PARTY THAT SERVICES OR PERSONAL DATA DELIVERED UNDER THE MSA WILL BE COMPILED FROM VARIOUS SOURCES, INCLUDING PUBLIC RECORDS, AND ARE PROVIDED "AS IS". NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE, DESIGN, CONDITION, QUALITY, CAPACITY, MATERIAL OR WORKMANSHIP ARE BEING MADE, AND ARE HEREBY SPECIFICALLY EXCLUDED, IT BEING EXPRESSLY AGREED THAT ALL SUCH RISK AS BETWEEN SERVICE PROVIDER AND AUTHORISED THIRD PARTY SHALL BE BORNE BY AUTHORISED THIRD PARTY. IN NO EVENT SHALL SERVICE PROVIDER BE LIABLE FOR ANY DAMAGES SUFFERED OR INCURRED BY AUTHORISED THIRD PARTY RESULTING FROM THE USE BY AUTHORISED THIRD PARTY OF THE SERVICES OR

PERSONAL DATA OR ANY DISRUPTION OF SERVICE OR DELAY IN PROVIDING THE SAME, WHETHER OR NOT AS A RESULT OF ANY FORCE MAJEURE. SERVICE PROVIDER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, OR FOR INCIDENTAL, SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES ARISING OUT OF THE PERFORMANCE OF THE MSA AND ANY APPLICABLE ADDENDUM, REGARDLESS OF WHETHER SUCH DAMAGES SHOULD BE SUSTAINED BY AUTHORISED THIRD PARTY OR CLIENT OR ANY OTHER PERSON OR ENTITY AND EVEN IF SERVICE PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

6. **Release from liability.** Client agrees that Service Provider and its affiliated companies, and all of their respective officers, directors, agents, employees and independent contractors shall be held harmless against all expense, damage or liability resulting from disclosure by Authorised Third Party, its officers, directors, employees, agents, or independent contractors, contrary to the terms of the MSA and any applicable Addendum of any information obtained from Service Provider. If Service Provider reasonably determines that Authorised Third Party is using, or is attempting to use, any Service or Personal Data in a manner contrary to the terms of the MSA and any applicable Addendum, Service Provider shall have, in addition to any other remedies, the right to equitable relief enjoining such action.

7. **Payment.** Client shall be invoiced for all charges incurred by Authorised Third Party for Services requested on behalf of Client, including applicable fees as well as charges resulting from Authorised Third Party's errors in inputting data, duplicate requests and errors in transmission.