First Advantage
A Symphony Technology Group Company

DATA PRIVACY ATTACHMENTS

A. PRIVACY SHIELD ONWARD TRANSFER ATTACHMENT

1. **Purpose of the Attachment.** Contractor provides professional services for Customer as mutually agreed upon between Customer and Contractor and further described in a separate agreement between the parties. This Attachment in particular covers the processing of Personal Data (as that term is defined in Section 2) by Contractor on behalf of First Advantage Background Services Corp. and/or its U.S. affiliated organizations which are self-certified pursuant to the EU-U.S. and/or Swiss-U.S. Privacy Shield frameworks pertaining to the employees of, or applicants for employment with, Customer's clients (a "Data Subject"), which may be securely accessed by or transferred to Contractor for the purpose of performing background screening and verification services.

2. **Definition of Personal Data.** In this Attachment, Personal Data shall include any data and information covered by the definition of personal data under the European Union General Data Protection Regulation (EU) 2016/679 ("GDPR"). As defined in the GDPR, Personal Data is any information relating to an identified or identifiable person (*i.e.* a Data Subject) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3. **Terms and Obligations**. The following regulates the transfer, processing, and use of Personal Data in order to ensure protection consistent with the EU-U.S. and/or Swiss-U.S. (as applicable) Privacy Shield Privacy Principles (collectively referred to herein as the "Privacy Shield Privacy Principles") which are set forth at http://www.privacyshield.gov and by reference are made a material part of this Attachment. Contractor agrees that:

   a. Contractor and any other parties acting under its authority shall process Personal Data only as directed by Customer for the limited and specified purposes identified by Customer, as authorized by the Data Controller/Data Subject.

   b. Contractor shall enter into a contract with all subcontractors and other third parties having access to Personal Data which shall require the subcontractor, or third party, to comply with the same data protection obligations as are required of Contractor by this Attachment.

   c. Contractor shall take reasonable and appropriate legal, organizational, and technical measures to protect Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, keeping in mind the risks involved in the processing and the nature of the Personal Data. In this context Contractor shall, upon Customer's request, and within a reasonable time, correct, delete, and/or block Personal Data from further processing and/or use.

   d. Contractor shall hold those of its employees with access to Personal Data accountable for violations of this Attachment and impose sanctions, which include, where appropriate, the possibility of termination of contracts and employment.

   e. Contractor shall process the Personal Data received from Customer in accordance with the relevant Privacy Shield Privacy Principles (found at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg); except that Customer shall remain responsible for responding to requests for access and enforcement.

   f. Contractor shall notify Customer promptly if (i) Contractor makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield Privacy Principles; and (ii) Contractor experiences a security breach where Contractor suspects or reasonably believes that Personal Data or any Customer Confidential Information (as that term is defined by the underlying services agreement) has been disclosed to or accessed by an unauthorized party. In the event of such a security breach, Contractor shall not notify any potentially affected consumers or other parties unless Customer authorizes such notification. If Customer authorizes notification to consumers and/or other parties, such notification shall be conducted in accordance with Customer's Information Security Breach Response and Notification Policy (applicable provisions available upon request) and applicable laws. It is Contractor's sole responsibility to determine its compliance obligations pursuant to applicable security breach laws, but Customer may elect to assist Contractor in its sole discretion.

   g. Contractor must ensure that email transmissions containing Personal Data are encrypted and that the Personal Data within such email transmissions is truncated or masked where possible.

   h. Contractor shall indemnify Customer, its subsidiaries and/or affiliated companies against any loss or liability to the extent loss or liability results from Contractor's breach of this Attachment, breach of applicable laws, or any security breach caused or arising from the actions or inactions of Contractor.

   i. EXCEPT AS EXPRESSLY PROVIDED HEREIN CUSTOMER SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONTINGENT, CONSEQUENTIAL, PUNITIVE, EXEMPLARY, SPECIAL OR SIMILAR DAMAGES, INCLUDING BUT NOT LIMITED TO, LOSS OF PROFITS WHETHER INCURRED AS A RESULT OF NEGLIGENCE OR OTHERWISE, IRRESPECTIVE OF WHETHER CUSTOMER HAS BEEN ADVISED OF THE POSSIBILITY OF THE INCURRENCE OF ANY SUCH DAMAGES. ANY LIABILITY DAMAGES CLAIMED BY CONTRACTOR AS INCURRED PURSUANT TO THIS AGREEMENT, INCLUDING AS A RESULT OF ANY NEGLIGENCE ON THE PART OF CUSTOMER, SHALL NOT EXCEED THE AMOUNT OF THE FEES CUSTOMER HAS PAID CONTRACTOR FOR THE SERVICES.

   j. Interpretation of this agreement shall be governed by the laws of the United States, specifically the state of Georgia, without reference to the conflict of laws principles thereof.

   k. If any provision of this Attachment is held to be unenforceable, the remaining provisions will be unaffected. Each provision of this Attachment, which provides for a limitation of liability or exclusion of remedies, is severable from and independent of any other provision.

First Advantage
A Symphony Technology Group Company

B. DATA PROTECTION ATTACHMENT

This Data Protection Attachment ("Attachment") forms part of the Agreement between Contractor (also herein referred to as the "Supplier" or "data importer") and Customer (also referred to as the "data exporter" or "First Advantage") to reflect the parties' agreement with respect to the Processing of Personal Data. Supplier enters into this Attachment on behalf of itself and, to the extent required under applicable Data Protection Law, in the name and on behalf of its authorised affiliates, if and to the extent that Supplier Processes Personal Data for which such authorised affiliates qualify as the Data Controller. In the course of providing the Services to Customer pursuant to the Agreement, Supplier may Process Personal Data on behalf of Customer who provides background screening services on behalf of its clients established as data controllers in the European Union/European Economic Area, and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Attachment to the Agreement Except where the context requires otherwise, references in this Attachment to the Agreement are to the Agreement as amended by, and including, this Attachment.

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Definitions

For the purposes of the clauses:

(a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

(b) "the data exporter" shall mean the controller who transfers the personal data;

(c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

(d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

(a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

(b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

(c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

(d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

(e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the

authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

(a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

(b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

(c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

(d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

(e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

(f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

(g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

(h) It will process the personal data, at its option, in accordance with:

(i) the data protection laws of the country in which the data exporter is established, or

(ii) the relevant provisions ([1]) of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data ([2]), or

(iii) the data processing principles set forth in Annex A.

(i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

(ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

(a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

(b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

(a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

(b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

(c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

(a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

(b) In the event that:

(i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

(ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

(v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

(c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

(d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

([1]) "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

([2]) However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.
6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.
8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   (a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject, and

   (ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   (b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

Data Subjects

The personal data transferred concern the following categories of data subjects:

Employees and prospective employees (candidates) of the data exporter's (or its affiliates') background screening services customers and/or investment managers who are expected to manage funds or strategies in which data exporter's customers are considering investing or has already invested

Purposes of the Transfer(s)

The transfer is made for the following purposes:

To perform background screening checks for employment purposes and/or perform due diligence services

Categories of Data

The personal data transferred concern the following categories of data:

As related to background screening services: 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. Past employment and positions held in other organizations, including fiduciary or Board of Directors responsibilities for a company;

As related to due diligence services: professional qualifications, registrations, and sanctions with professional bodies; Court records and/or financial information relating to bankruptcy and collection matters, financial judgments, litigation; Criminal proceedings, convictions and involvement in litigation, including civil suits where the subject was either a plaintiff or defendant; Media information; Patents and other intellectual property; Corporate records.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Employees, agents, and subprocessors of the data importer who are authorised to receive the data and who need access to the information in order to perform services for the data exporter

Sensitive Data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

N/A

Data protection registration information of exporter (where applicable)

Additional useful information (storage limits and other relevant information)

GDPR TERMS

1. Definitions

1.1 In this Attachment, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws to which First Advantage is subject (including EU Data Protection Laws); and (b) any other applicable law to which First Advantage is subject (including Data Protection Laws);

1.1.2 "**Contracted Processor**" means Supplier or a Subprocessor;

1.1.3 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country that has established legislation implementing or supplementary to the requirements of the EU Data Protection Laws;

1.1.4 "**EEA**" means the European Economic Area;

1.1.5 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.6 "**GDPR**" means EU General Data Protection Regulation, Regulation (EU) 2016/679;

1.1.7 "**Personal Data**" means any information relating to an identified or identifiable natural person located within the EEA or Switzerland, as this is defined under Applicable Laws;

1.1.8 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Supplier for First Advantage pursuant to the Agreement;

1.1.9 "**Subprocessor**" means any person (including any third party and any Supplier Affiliate, but excluding an employee of Supplier or any of its sub-contractors) appointed by or on behalf of Supplier or any Supplier Affiliate to Process Personal Data on behalf of any First Advantage affiliate in connection with the Agreement; and

1.1.10 **"Supplier"** means the data importer as defined in the Standard Contractual Clauses to which this Attachment is attached;

1.1.11 "**Supplier Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Supplier, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Personal Data

2.1 Supplier and each Supplier Affiliate shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Personal Data; and

2.1.2 not Process Personal Data other than on the relevant First Advantage instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Supplier or the relevant Supplier Affiliate shall to the extent permitted by Applicable Laws inform the relevant First Advantage affiliate of that legal requirement before the relevant Processing of that Personal Data.

3. Supplier Personnel

Supplier and each Supplier Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know or access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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, Supplier and each Supplier Affiliate shall in relation to the Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Applicable Laws (e.g. Article 32(1) of the GDPR). At a minimum, these measures shall include without limitation:

4.1.1 access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing Personal Data to unauthorized individuals who may seek to obtain this information through fraudulent means;

4.1.2 access restrictions at physical locations containing Personal Data, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

4.1.3 encryption of electronic Personal Data, including while in transit, or in storage on networks or systems to which unauthorized individuals may have access;

4.1.4 procedures designed to ensure that information system modifications are consistent with the information security measures;

4.1.5 dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to Personal Data;

4.1.6 monitoring systems and procedures to detect actual and attempted attacks on or intrusions into information systems;

4.1.7 response programs that specify actions to be taken when Supplier detects unauthorized access to information systems, including immediate reports to First Advantage;

4.1.8 measures to protect against destruction, loss or damage of Personal Data due to potential environmental hazards, such as fire and water damage or technological failures;

4.1.9 training of staff to implement the information security measures;

4.1.10 regular testing of key controls, systems and procedures of the information security measures by independent third parties or staff independent of those that develop or maintain the security measures; and

4.1.11 reporting to First Advantage on the results of its audit evaluations of Supplier's information security systems and procedures.

4.2 In assessing the appropriate level of security, Supplier and each Supplier Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Subprocessing**

5.1 First Advantage authorises Supplier and each Supplier Affiliate to appoint (and permit each Subprocessor appointed in accordance with this section to appoint) Subprocessors in accordance with this section and any restrictions in the Agreement.

5.2 Regardless of the Subprocessor appointed, Supplier, and each Supplier Affiliate, shall remain liable for the actions of any Subprocessor under the terms of the Agreement.

5.3 Supplier and each Supplier Affiliate may continue to use those Subprocessors already engaged by Supplier or any Supplier Affiliate as at the date of this Attachment, subject to Supplier and each Supplier Affiliate in each case as soon as practicable meeting the obligations set out in this section.

5.4 Supplier shall give First Advantage prior written notice of the appointment of any new Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within thirty (30) days of receipt of that notice, First Advantage notifies Supplier in writing of any objections (on reasonable grounds) to the proposed appointment neither Supplier nor any Supplier Affiliate shall appoint (nor disclose any Personal Data to) the proposed Subprocessor except with the prior written consent of First Advantage.

5.5 With respect to each Subprocessor, Supplier or the relevant Supplier Affiliate shall:

5.5.1 before the Subprocessor first Processes Personal Data carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Personal Data required by this Attachment;

5.5.2 ensure that the arrangement between (a) Supplier, or (b) the relevant Supplier Affiliate, or (c) the relevant intermediate Subprocessor; and hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Personal Data as those set out in this Attachment;

5.5.3 provide to First Advantage for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Attachment) as First Advantage may request from time to time.

5.6 Supplier and each Supplier Affiliate shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Personal Data carried out by that Subprocessor, as if it were party to this Attachment in place of Supplier.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Supplier and each Supplier Affiliate shall assist each First Advantage affiliate by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of First Advantage's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Supplier shall:

6.2.1 promptly notify First Advantage if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of First Advantage or the relevant First Advantage Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Supplier shall to the extent permitted by Applicable Laws inform First Advantage of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

7.1 Supplier shall notify First Advantage without undue delay upon Supplier or any Subprocessor becoming aware of a Personal Data Breach affecting Personal Data, providing First Advantage with sufficient information to allow each First Advantage affiliate to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Supplier shall cooperate with First Advantage and each First Advantage affiliate and take such reasonable commercial steps as are directed by First Advantage to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Supplier and each Supplier Affiliate shall provide reasonable assistance to each First Advantage affiliate and/or First Advantage customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which First Advantage reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Personal Data

9.1 Except as otherwise permitted under this Attachment, Supplier and each Supplier Affiliate shall promptly and in any event within thirty (30) days of the date of termination of any Services involving the Processing of Personal Data (the "**Termination Date**"), delete and procure the deletion of all copies of those Personal Data.

9.2 Subject to section 9.3 below, First Advantage may in its absolute discretion by written notice to Supplier within thirty (30) days of the Termination Date require Supplier and each Supplier Affiliate to (a) return a complete copy of all Personal Data to First Advantage by secure file transfer in such format as is reasonably notified by First Advantage to Supplier; and (b) delete and procure the deletion of all other copies of Personal Data Processed by any Contracted Processor. Supplier and each Supplier Affiliate shall comply with any such written request within thirty (30) days of the Termination Date.

9.3 Each Contracted Processor may retain 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 Supplier and each Supplier Affiliate shall ensure the

confidentiality of all such Personal Data and shall ensure that such Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 Supplier shall provide written certification to First Advantage that it and each Supplier Affiliate has fully complied with this section within ninety (90) days of the Termination Date.

10. Audit rights

10.1 Except as otherwise provided in this Attachment, Supplier and each Supplier Affiliate shall make available to First Advantage, on request, all information necessary to demonstrate compliance with this Attachment, and shall allow for and contribute to audits, including inspections, by First Advantage, its customer, or an auditor mandated by First Advantage or mutually agreed to by First Advantage and its customer, in relation to the Processing of the Personal Data by the Contracted Processors.

10.2 Information and audit rights of First Advantage only arise under this section to the extent that the underlying Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

10.3 First Advantage shall give Supplier or the relevant Supplier Affiliate reasonable notice of any audit or inspection to be conducted under this Attachment, with such audit being upon a mutually agreed scope and time. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and First Advantage undertaking an audit has given notice to Supplier or the relevant Supplier Affiliate that this is the case before attendance outside those hours begins; or

10.3.2 for the purposes of more than one audit or inspection, in respect of each Contracted Processor, in any calendar year, except for any additional audits or inspections which:

10.3.2.1 First Advantage reasonably considers necessary because of genuine concerns as to Supplier's or the relevant Supplier Affiliate's compliance with this Attachment; or

10.3.2.2 First Advantage or its customer is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where First Advantage has identified its concerns or the relevant requirement or request in its notice to Supplier or the relevant Supplier Affiliate of the audit or inspection.

11. General Terms

Order of precedence

11.1 In the event of inconsistencies between the provisions of this Attachment and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Attachment, the provisions of this Attachment shall prevail.

Changes in Data Protection Laws, etc.

11.2 First Advantage may propose any other variations to this Attachment which First Advantage reasonably considers to be necessary to address the requirements of any Data Protection Law.

12. Disaster Recovery

12.1 Supplier shall provide business continuity, disaster recovery, pandemic and backup capabilities and facilities acceptable to First Advantage, through which Supplier will be able to perform its obligations hereunder with minimal disruptions or delays. Supplier shall provide to First Advantage copies of its written business continuity, disaster recovery, and pandemic and backup plan(s). Supplier shall comply with all such plans and promptly notify First Advantage of any material changes to such plans, provide First Advantage with copies of such materially changed plans and obtain First Advantage's approval of such material changes.

First Advantage
A Symphony Technology Group Company

C. SECURITY OBLIGATIONS ATTACHMENT

Recitals

1. Contractor provides professional services for Customer as mutually agreed upon between Customer and Contractor and further described in a separate agreement between the parties ("Agreement").

2. Customer may provide Contractor with Sensitive Consumer Information (defined below) regarding natural persons to enable Contractor to perform services pursuant to the Agreement.

3. Customer and Contractor desire to clarify Contractor's security obligations relating to Sensitive Consumer Information.

As such, the parties to this Attachment agree pursuant to the provisions set forth below and Contractor hereby certifies that it will comply with the provisions set forth below.

1. DEFINITIONS.

As used in this Attachment, the following capitalized terms shall have the meanings given to them below:

"Sensitive Consumer Information" means an individual's first name or first initial and last name in combination with any one or more of the following items: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account, or as otherwise defined by applicable federal or state statute or regulation as personally identifiable information.

"Damages" means any and all assessments, judgments, claims, liabilities, losses, costs, damages, or expenses, including, but not limited to, interest, penalties, and reasonable attorneys' fees, expenses, and disbursements in connection with an action, suit or proceeding.

"Indemnified Customer Entities" means Customer and each and every current, former and future officer, director, agent, and employee of Customer.

2. NOTIFICATION OF SECURITY BREACH.

a. In the event of any actual or suspected security breach that Contractor either suffers or learns of that compromises or is likely to compromise Sensitive Consumer Information (e.g., physical trespass on a secure facility, computing systems intrusion/hacking, loss/theft of a PC (laptop or desktop), loss-theft of printed materials, etc.) (collectively, a "Security Breach"), Contractor will promptly notify Customer security personnel of such Security Breach and will immediately coordinate with Customer security personnel to investigate and remedy the Security Breach, as directed by Customer security personnel. Except as may be permitted by applicable law, Contractor agrees that it will not inform any third party of any such Security Breach without Customer's prior written consent; however, if such disclosure is required by applicable law, Contractor agrees to work with Customer regarding the content of such disclosure so as to minimize any potential adverse impact upon Customer and its clients and customers. Contractor also agrees to provide notification to those individuals affected by the Security Breach in the event the Security Breach was caused by or arose from the actions or inactions of Contractor.

b. Without limiting Contractor's indemnification or other obligations or liabilities under the Agreement, Contractor shall indemnify the Indemnified Customer entities and hold each of them harmless from and against, and shall assume liability for, any and all Damages suffered, paid, or incurred by any Indemnified Customer Entity resulting from any breach by Contractor of its representations, covenants, obligations or conditions under this Attachment or from any Security Breach caused by or arising from the actions or inactions of Contractor.

3. ACCESS SECURITY REQUIREMENTS.

Contractors shall take precautions to secure any system or device used to access Sensitive Consumer Information provided by Customer. To that end, the following requirements have been established:

a. Contractor's account number and password to access Sensitive Consumer Information provided by Customer must be protected in such a way that this sensitive information is known only to key personnel with a need to know in order to complete the services for Customer. Under no circumstances should unauthorized persons have knowledge of these passwords. The information should not be posted in any manner within Contractor's facility. Do not provide account numbers or passwords to anyone.

b. Any system access software Contractor may use, whether developed by Contractor or purchased from a third party vendor, must have the account number and password "hidden" or embedded so that the password is known only to supervisory personnel. Each user of Contractor's system access software must then be assigned unique log-on passwords. Develop strong passwords that are:
   - Not easily guessable (i.e. user name or company name, repeating numbers and letters or consecutive numbers and letters).
   - Obtain a minimum of eight (8) alpha/numeric characters for standard user accounts.
   - Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
   - Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.

c. Contractor must request that account number and/or password be changed immediately when:
   - Any system access software is replaced by another system access software or
   - is no longer used;
   - The hardware on which the software resides is upgraded, changed or disposed of.

d. Contractor's account number and passwords are not to be discussed by telephone to any unknown caller, even if the caller claims to be an employee.

e. Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.

f. The ability to obtain Sensitive Consumer Information from Customer must be restricted to a few key personnel with a need to know to complete Contractor's services to Customer.

g. Any terminal devices used to obtain Sensitive Consumer Information should be placed in a secure location within your facility. Access to the devices should be difficult for unauthorized persons.

h. Any devices/systems used to obtain Sensitive Consumer Information should be turned off and locked after normal business hours, when unattended by Contractor's key personnel.

i. Sensitive Consumer Information should not be downloaded onto a laptop computer or other mobile device, without the appropriate best security and encryption standards common to the industry.

j. Hard copies and electronic files of Sensitive Consumer Information are to be secured within Contractor's facility and protected against release or disclosure to unauthorized persons.

k. Hard copies of documents containing Sensitive Consumer Information are to be shredded or destroyed, rendered unreadable, when no longer needed and when it is permitted to do so by applicable regulations(s). Such shredding, destruction and unreadable rendering shall be done in compliance with the document destruction rules as promulgated by the Fair Trade Commission pursuant to the Fair and Accurate Credit Transaction Act ("Document Destruction Rules").

l. Electronic files containing Sensitive Consumer Information will be completely erased or rendered unreadable when no longer needed and when destruction is permitted by applicable regulation(s). Such erasing, deleting, and unreadable rendering shall be done in compliance with the Document Destruction Rules.

4. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

a. Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.

b. Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

c. Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
   - Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
   - If Contractor suspects an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
   - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.

d. Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
   - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
   - If Contractor suspects actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
   - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from Contractor's computers.
   - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If Contractor's computers have unfiltered or unblocked access to the Internet (which

prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

5. PROTECT SENSITIVE CONSUMER INFORMATION

a. Develop and follow procedures to ensure that Sensitive Consumer Information is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)

b. Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

c. Only open email attachments and links from trusted sources and after verifying legitimacy.

6. MAINTAIN AN INFORMATION SECURITY POLICY

a. Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.

b. The FACTA Disposal Rules requires implementation of appropriate measures to dispose of any Sensitive Consumer Information that will protect against unauthorized access or use of that information.

c. Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within Contractor's organization.

7. BUILD AND MAINTAIN A SECURE NETWORK

a. Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

b. Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

c. Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.

d. Any standalone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

e. Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.

f. Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

8. REGULARLY MONITOR AND TEST NETWORKS

a. Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).

b. Use current best practices to protect telecommunications systems and any computer system or network device(s) used to access credit reporting agency systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:
   - protecting against intrusions;
   - securing the computer systems and network devices;
   - protecting against intrusions of operating systems or software.

9. STAFFING AND SCREENING

Contractor shall ensure that personnel are qualified, empowered and resourced to execute their duties. Contractor shall also ensure proper screening of individuals that come in contact with Sensitive Consumer Information. For Contractor personnel located in the United States, the background investigation must include at least: (i) social security number verification; (ii) a criminal records search going back at least seven (7) years; (iii) multi-jurisdictional criminal court search and (iv) for individual with access to sensitive personally identifiable information, employment background screening that meets applicable local best practices. Outside the United States, Contractor must comply with applicable local best practices for employment background screening for individuals with access to sensitive personally identifiable information. Contractor must also re-credential personnel periodically according to best practices.

In the event that any of Contractor's personnel is found to have been convicted of any felony, crime of dishonesty, breach of trust, etc., that alone will not necessarily preclude an individual from engaging with Customer. Rather, Contractor must consider a number of factors, including, but not limited to, the nature and basis of the conviction, the relationship between the conviction and the responsibilities the individual will have with Customer, what Customer databases or systems the individual will have access to, what level of access the individual will have at Customer facilities, the time passed since conviction, any inconsistency or omissions of information supplied by the Contractor's personnel, the conduct of the individual since the conviction, evidence of rehabilitation and the individual's employment history.

10. SECURITY STANDARDS

Contractor agrees to abide by industry best practices to maintain the security, privacy and integrity of any Sensitive Consumer Information provided by Customer to Contractor pursuant to this addendum or any Service Arrangements. Contractor must maintain adequate records of and regularly monitor its implementation of and compliance with the obligations set forth herein.

Furthermore, Contractor agrees to cooperate with and comply with, in a timely manner, any procedures or requests made by Customer, including without limitation any vetting or credentialing processes to help minimize any security risk that may exist or could potentially exist.

11. TERM OF SERVICE ARRANGEMENTS.

Without limiting any of Customer's existing termination or other rights under the Agreement, Customer may terminate the service arrangements with Contractor immediately upon Contractor's breach of any of its representations, covenants, obligations, or conditions under this Attachment or from any Security Breach caused by or arising from the actions or inactions of Contractor.

12. EFFECT

In the event of a conflict between the Agreement and this Attachment, this Attachment shall control matters relating to a Security Breach, notwithstanding any other provisions of the Agreement. All other terms and conditions of the Agreement shall remain in full force and effect. The validity of any provision hereof shall in no way affect or invalidate the remainder of such Agreement or this Attachment.

13. SURVIVAL

All sections of this Attachment with the exception of Section 5 of this Attachment shall survive the termination of this Attachment and of the Agreement.