EQUIFAX DIGITAL SOLUTIONS DATA PROTECTION ADDENDUM

Equifax and Client acknowledge that the EDS Services will involve the Processing of Personal Information included within any Inquiry. This Data Protection Addendum ("**DPA**") is intended to comply with the parties' obligations under the Applicable Law, including without limitation the applicable Privacy Laws, with respect to the Processing of Personal Information pursuant to the EDS Schedule. All references to "**Equifax**" shall refer to such Equifax Affiliate that is providing the EDS Services to Client. The parties are individually referred to as a "**Party**" or collectively as "**Parties**". All capitalized terms used but not defined in this DPA shall have the meanings given them in the EDS Schedule. Any conflict between this DPA and the EDS Schedule shall be resolved in favor of this DPA.

1. Definitions.

1.1. "**Applicable Law**" means all applicable laws (including those arising under common law), statutes, cases, ordinances, constitutions, regulations, treaties, rules, codes, ordinances and other pronouncements having the effect of law of the United States, any foreign country or any domestic or foreign state, county, city or other political subdivision, including those promulgated, interpreted or enforced by any governmental authority where Client does business, including Privacy Laws. References to "**Applicable Law**" mean Applicable Law as may be amended or supplemented.

1.2. "**Controller**" or "**Business**" have the meanings given within the applicable Privacy Laws.

1.3. "**Data Subject**" has the meaning given to that term in the applicable Privacy Law.

1.4. "**EU GDPR**" means the General Data Protection Regulation (EU) 2016/679.

1.5. "**GDPR**" means the EU GDPR or the UK GDPR (as applicable).

1.6. "**Personal Information**" or "**Personal Data**" means any information reasonably relating to an identified or identifiable natural person (an identifiable natural person is one who can be identified, directly or indirectly) and provided or made available by Client to Equifax and/or collected or otherwise obtained by Equifax in connection with the performance of the EDS Services by Equifax to Client or as otherwise defined in applicable Privacy Laws, including but not limited to the information set forth in **Annex 1**.

1.7. "**Privacy Authority**" shall mean the relevant supervisory authority with responsibility for the promulgation or enforcement of the Privacy Laws.

1.8. **"Privacy Laws**" means all Applicable Laws relating to the privacy, confidentiality, retention or security of Personal Information including, but not limited to, (i) the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020, and any binding regulations promulgated thereunder (collectively, "**CCPA**"), Virginia's Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, Connecticut's An Act Concerning Personal Data Privacy and Online Monitoring; (ii) the UK Data Protection Laws; (iii) the EU GDPR; (iv) Switzerland Data Protection Laws; (v) the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI2003/2426); (vi) any additional privacy laws that may come into effect from time to time governing the use of Personal Information; and (vii) any regulations, guidance, or statutory codes issued by the relevant Privacy Authority that implement any of the above laws.

1.9. "**Process**", "**Processing**" or "**Processed**" means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, alteration, use, access, disclosure, copying, transfer, storage, deletion, alignment or combination, restriction, adaptation, retrieval, consultation, destruction, disposal, or other use of Personal Information.

1.10. "**International Data Transfer Appendix**" the Appendix set out as Annex 3 of this DPA detailing authorized transfers of Personal Information by Equifax outside the European Economic Area, United Kingdom, and Switzerland in connection with one or more of the EDS Services.

1.11. **"Switzerland Data Protection Laws**" means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in Switzerland, including the Federal Act on Data Protection of 19 June 1992 as revised as of 25 September 2020 (the "**FADP**").

1.12. "**UK Data Protection Laws**" shall mean all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

1.13. "**UK GDPR**" has the meaning given to it in section 3(10) (as supplemented by section 205(4) of the Data Protection Act 2018.

2. Roles of Parties; Scope of Use. For the purposes of the applicable Privacy Laws, Equifax and the Client shall be independent Controllers of the Personal Information that it collects or Processes pursuant to the EDS Schedule. The Parties agree that (i) they are not joint Controllers of any Personal Information; (ii) each Party shall be individually and separately responsible for complying with the obligations that apply to it as a Controller under the applicable Privacy Law; and (iii) each Party will individually determine the purposes and means of its processing of Personal Information. Nothing in this Section 2 modifies any restrictions applicable to either party's rights to use the Personal Information as set out in the EDS Schedule and Equifax will use the Personal Information solely and exclusively as permitted under the EDS Schedule. This DPA does not apply to any information that is not classified as Personal Information or Personal Data or comparable terms under any Privacy Laws, including but not limited to information that is classified as aggregate consumer information or deidentified information in compliance with applicable Privacy Laws.

3. Obligations of the Parties.

3.1. Each Party shall comply with its own obligations under the applicable Privacy Laws, subject to compliance with Section 3.2.

3.2. Certain EDS Services require Client to deploy a Device Data Collector (as defined in the Documentation available at developer.kount.com, "**DDC**") on Client's website(s). The DDC is maintained by Kount Inc., an Equifax Affiliate ("Kount"). Client acknowledges and agrees that Equifax does not have any direct interaction with Client's consumers. Accordingly, if deployment of the DDC is required, and if required by the applicable Privacy Laws, then Client shall ensure that:

3.2.1 users of Client's website(s) have given consent to the use of cookies before the deployment of the DDC; and

3.2.2 a copy of or link to Kount Inc.'s privacy policy is made available to users of Client's website(s).

3.3. To facilitate compliance with any cookie disclosure or consent laws that may apply to Client, Equifax provides the following information regarding the DDC's use of cookies:

Source	Examples	Cookie description	Duration
Kount	ss Cdn.{dynamic_name}.{dynamic_identifier} applicationUserProfileSettings	Cookies from Kount are set for the purposes of fraud detection. These cookies store unique values to help identify and protect against fraud. Additional information regarding Kount's use of cookies is available at: https://kount.com/legal/privacy-policy	90 to 365 days

3.4. Each Party will maintain a public-facing privacy policy on its website that complies with the applicable Privacy Laws.

3.5. To the extent either party receives Cardholder Data (as defined in the Payment Card Industry Data Security Standard ("**PCI DSS**"), as amended or replaced from time to time)) or any other data covered under the PCI DSS (collectively, "**PCI Data**"), such party will ensure that it has in place, and shall maintain for as long as it has possession of and/or access to PCI Data, a compliant system for transmission, reception, storage, and use of PCI Data. If applicable, Equifax and Client each will ensure that it can now and shall continue to be able to provide evidence that it has been deemed PCI Compliant by the PCI SSC and shall maintain such designation during the time period that party has possession of and/or access to PCI Data. If applicable, Client will provide annual attestation that it is compliant with the current PCI DSS.

4. Security; Notice; Cooperation.

4.1. Each Party shall maintain (and require its subprocessors or subcontractors to maintain) reasonable and appropriate technical and organizational measures for the protection of the security, confidentiality, and integrity of Personal Information (including protection against security incidents impacting Personal Information) and at a minimum employ the technical and organizational measures set out in Annex 2 below. In addition, each Party will treat Personal Information with strict confidence and take all reasonable steps to ensure that persons it employs and/or persons engaged at its place(s) of business who will process Personal Information comply with this DPA.

4.2. Unless otherwise prohibited by Applicable Law, a Party will provide the other Party written notification promptly, and in no event no later than 72 hours, after either (i) confirming any accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, Personal Information; or (ii) becoming aware of any complaint, inquiry, or request from an individual or government or regulatory agency regarding Personal Information. Each Party will refrain from notifying or responding to any data subject, government or regulatory agency, or other third party, for or on behalf of the other Party, unless requested in writing by the other Party to do so, except as and when otherwise required by Applicable Law. Both Parties agree and acknowledge that if a Party receives a request from a government or regulatory agency, that Party may share the terms of this DPA, the EDS Schedule, and other information to demonstrate compliance with this DPA or Applicable Law. The Parties agree to reasonably cooperate and assist each other in relation to any regulatory or governmental request, complaint, or investigation concerning the Personal Information shared between the Parties.

5. Individual Rights Requests. Each Party will separately process any requests for Data Subjects to exercise their rights with regard to the Personal Information. If a Data Subject submits a request with respect to the Processing of Personal Data that is shared between the Parties, including any opt out or deletion requests, the Parties will collaborate in good faith to honor such requests as required by applicable Privacy Law.

6. Cross-Border Transfers of Personal Information.

6.1. Where Personal Information originating in a territory is transferred to or Processed by a Party in another territory, and the applicable Privacy Law requires certain measures to be implemented prior to such transfer, Equifax and Client will implement such measures as shall be mutually agreed upon.

6.2. For transfers of Personal Information from the European Economic Area, United Kingdom, or Switzerland to territory that is not subject to an adequacy determination by the European Commission, the UK, or Swiss Privacy Authority (as applicable) ("**Restricted Transfer**"), then the Standard Contractual Clauses ("**SCCs**") annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 are hereby incorporated by references set out in the International Data Transfer Appendix attached hereto and form an integral part of the EDS Schedule.

7. Data Protection Impact Assessment. Upon Client's written request and at Client's expense, Equifax shall provide Client with reasonable cooperation and assistance as needed and appropriate to fulfill Client's obligations under the

Applicable Law to carry out a data protection impact assessment related to Client's use of the EDS Services.

8. **Audit Rights**. Equifax shall conduct independent third-party reviews of its privacy and data security measures against industry leading frameworks (e.g., PCI-DSS, SOC 2 Type 2, ISO 27001) at least once per year as long as Equifax Processes Personal Information and, upon Client's written request, provide a summary of such reports to Client.

9. **Allocation of Costs**. Except as otherwise noted herein, each Party shall bear its own costs in relation to its obligations under this DPA.

10. **Liability**. The Parties' liability under or in connection with this DPA is subject to the exclusions and limitations of liability set out in the Parties' Agreement.

11. **General**. If any part of this DPA is held unenforceable, the DPA will be interpreted with the unenforceable portion of the DPA deleted, and the validity of all remaining parts will not be affected. Except for the changes made by this DPA, the EDS Schedule remains unchanged and in full force and effect.

ANNEX 1: Subject Matter and Details of Processing

PARTIES		
	Client	**Equifax**
Name:	As set forth in the Ordering Document	Equifax Affiliate
Contact details for data protection:	As set forth in the Ordering Document	privacy@equifax.com
Activities:	Operation of website	Fraud and identity verification services.
Role:	Exporter; Controller	Importer; Controller

SUBJECT MATTER AND DETAILS OF TRANSFER	
Nature and Purpose:	To provide the EDS Services in accordance with the EDS Schedule.
Categories of Data Subjects:	Client's current and former customers and/or others that interact with Client's website, mobile site, or application where the EDS Services are utilized.
Categories of Personal Data:	Any Personal Data provided to Equifax under the EDS Schedule, but may include: **Personal details**, including any information that identifies the Data Subject, including name, address, contact details (including email address, telephone details and other contact information). **Payment details**, including bank account number, credit card number, debit card number, basket contents, or any other financial information. **Technological details**, such as internet protocol (IP) addresses, unique identifiers and numbers (including unique identifier in tracking cookies or similar technology), pseudonymous identifiers, precise and imprecise location data, internet / application / program activity data, and device IDs and addresses.
Categories of Special or Sensitive Data	None.
Duration:	For the period determined in accordance with the EDS Schedule and DPA.
Frequency:	Continuous.

ANNEX 2: Technical and Organizational Measures

1. **Written Information Security Program**. Implement, maintain and comply with written information security policies and procedures designed to protect the confidentiality, availability and integrity of Personal Data and any systems that store or otherwise process it, which are: (a) aligned with an industry-standard control framework (e.g., NIST SP 800-53, ISO 27001, SOC 2 Type 2, CIS Critical Security Controls); (b) approved by executive management; (c) reviewed and updated at least annually; and (d) communicated to all personnel with access to Personal Data. Assign to an individual or a group of individuals the responsibility for developing, implementing, and managing the organization's written information security program.
2. **Risk Assessment**. Maintain risk assessment procedures for the purposes of periodic review and assessment of risks to the organization, monitoring and maintaining compliance with the organization's policies and procedures and reporting the condition of the organization's information security and compliance to internal senior management.
3. **Personnel Training**. Train personnel to maintain the confidentiality, integrity, availability and security of Personal Data, consistent with the terms of the EDS Schedule and applicable Privacy Laws.
4. **Vendor Management**. Conduct reasonable due diligence and monitoring to ensure subcontractors are capable of maintaining the privacy, confidentiality, security, integrity and availability of Personal Data.
5. **Access Controls**. Maintain logical access controls designed to limit access to Personal Data and relevant information systems only to authorized personnel and third parties (e.g., granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job functions occur).
6. **Secure User Authentication**. Maintain password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that passwords controlling access to Personal Data must: (a) meet industry standard complexity requirements; and (b) be stored securely in accordance with industry best practices.
7. **Incident Detection and Response**. Maintain policies and procedures to detect and respond to actual or reasonably suspected Security Incidents and encourage the reporting of such incidents.
8. **Encryption**. Apply industry standard encryption to Personal Data: (a) stored on any medium (i.e., laptops, mobile devices, portable storage devices, file servers and application databases); and (b) transmitted across any public network (such as the Internet) or wirelessly.
9. **Network Security.** Implement industry standard network security controls such as up-to-date firewalls, layered DMZs, updated intrusion detection/prevention systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
10. **Vulnerability Management**. Implement vulnerability management, threat protection technologies and scheduled monitoring procedures to detect, assess, mitigate, remove and protect against new and existing security vulnerabilities and threats, including viruses, bots and other malicious code.

11. **Change Control**. Follow change management procedures and implement tracking mechanisms designed to test, approve and monitor all changes to technology and information assets.
12. **Physical Security**. Implement and maintain appropriate systems to restrict access to its premises, which shall be monitored.
13. **Business Continuity and Disaster Recovery**. Maintain business continuity and disaster recovery policies and procedures designed to maintain service and recover from foreseeable emergency situations or disasters.

ANNEX 3: International Data Transfer Appendix ("IDTA")

1 **Scope**. This IDTA only applies to Restricted Transfers as defined in Section 6.2 of the DPA.

2 Restricted Transfer.

2.1 The parties agree that, as Equifax is located in or otherwise Processing Protected Data in a territory outside of the European Economic Area, United Kingdom, or Switzerland, there will be a Restricted Transfer. A Restricted Transfer may only take place subject to the terms of this IDTA.

2.2 In the case of the Restricted Transfer, the parts of this IDTA that will apply depend upon whether the Restricted Transfer is governed by the EU GDPR, the UK GDPR, or the FADP as follows:

2.2.1 **EU GDPR**. If the Personal Information is transferred from the European Economic Area, the SCCs apply as follows:

1.1.1.1 the roles of 'data exporter' and 'data importer' are set out in Annex 1 to the DPA;

1.1.1.2 the Module One terms apply;

1.1.1.3 in Clause 7, the optional docking clause applies;

1.1.1.4 in Clause 11, the optional language does not apply;

1.1.1.5 in Clause 18(b), disputes will be resolved before the courts of Ireland;

1.1.1.6 Annex I.A and I.B are deemed complete with the information in Annex 1 to the DPA.

1.1.1.7 in Annex I.C and Clause 13(c), the Irish Data Protection Commissioner ("**DPC**") will act as the competent supervisory authority; and

1.1.1.8 Annex II, is deemed complete with the information set out in Annex 2 to the DPA.

1.1.2 **UK GDPR**. If the Personal Information is transferred from the United Kingdom, the SCCs apply as amended by Part 2 of the UK Addendum[1] to the SCCs, and Part 1 is deemed completed as follows:

1.1.2.1 Table 1, the details of the parties are set out in Annex 1 to the DPA;

1.1.2.2 Table 2, the selected modules and clauses are set out in Sections 2.2.1 of this IDTA, and the Personal Information from Importer **is** combined with Personal Information collected by Exporter;

1.1.2.3 Table 3, the appendix information is deemed complete with the information set out in Annex 1 and Annex 2 of the DPA; and

1.1.2.4 Table 4, 'Importer' and 'Exporter' are both selected.

1.1.3 **FADP**. If the Personal Information transferred from Switzerland, the SCCs apply as set out in Section 2.2.1 of this IDTA with the following modifications:

1.1.3.1 references to 'Regulation (EU) 2016/679' and its specific articles are read as references to the FADP and its equivalent article or section;

1.1.3.2 References to "EU", "Union", or "Member State" are replaced with "Switzerland";

1.1.3.3 Annex 1.C and Clause 13(a) are not used, and the 'competent supervisory authority' is the Swiss Federal Data Protection Information Commissioner ("**FDPIC**") or, if the transfer is subject to both the Swiss DPA and the GDPR, the FDPIC (insofar as the transfer is governed by the Swiss DPA) or the DPC (insofar as the transfer is governed by the GDPR);

1.1.3.4 references to the 'competent supervisory authority' and 'competent courts' are replaced with the 'FDPIC' and 'applicable courts of Switzerland';

1.1.3.5 in Clause 17, the SCCs are governed by the laws of Switzerland;

1.1.3.6 in Clause 18(b), disputes will be resolved before the competent Swiss courts;

1.1.3.7 the SCCs also protect the data of legal entities until entry into force of the revised FADP.

2 Conflicts. It is not the intention of either party to contradict or restrict any of the provisions set out in the SCCs or the UK Addendum, accordingly, if and to the extent that any provision of this IDTA conflicts with the SCCs or the UK Addendum, the SCC's and the UK Addendum (as applicable) will prevail to the extent of such conflict.

[1] UK Addendum refers to the UK's 'International Data Transfer Addendum to the EU Commission Standard Contractual Clauses' issued by the Information Commissioner's Office for parties making Restricted Transfers ("**UK Addendum**")