RECENT UPDATES

- The Equifax Customer Licence (ECL) forms a specific agreement that applies in addition to ASPL's usual Terms and Conditions of Sale (T&Cs), End-User Licence Agreement (EULA), Cloud Service Agreement (CSA) and Privacy Policy (the "Core Policies").
- The ECL only applies in relation to TaxCalc Customers who purchase or use the AML Identity Checking Service. The ECL entirely replaces the previous specific "EQUIFAX TAXCALC END USER TERMS AND CONDITIONS".
- Please read thoroughly if you are purchasing or intending to contuinue use of the AML Identity Checking Service.

Equifax Customer Licence: Anti-Money Laundering Identity Checking Service Only (2020-01-29)

1 ABOUT THIS EQUIFAX CUSTOMER LICENCE

1.1. In this Equifax Customer Licence, expressions defined in the Core Polices and used in this variation agreement have the meaning set out in the Core Policies, unless otherwise defined or amended below:

- "**You**" means You the customer who is using the Anti-Money Laundering Identity Checking Service;
- "**Core Policies**" means the Terms and Conditions of Sale (T&Cs), the End-User Licence Agreement (EULA), the Cloud Service Agreement (CSA) and the Privacy Policy (the "Core Policies");
- "**Party**" means either You; or Equifax Limited; or Acorah Software Products Limited; and together the "**Parties**";
- "**Equifax**" means Equifax Limited, a company incorporated in England and Wales (Registration Number: 02425920) and whose principal place of business is 1 Angel Court, London, United Kingdom, EC2R 7HJ; and
- "**this Licence**", "**ECL**" means this Equifax Customer Licence.
- "**External Party**" means either You; or Acorah Software Products Limited.
- "**the AML Service**" means the Anti-Money Laundering Identity Checking Service, provided by Equifax and sold by Acorah Software Products Limited as Reseller.
- "**the Reseller**" means Acorah Software Products Limited.
- "**CRAIN**" means the Credit Reference Agency Information Notice, as referenced in Section 1.4.1 of Attachment 4 (the Data Protection Policy).

1.2. This Licence commences as of the date of your agreement to this Licence. At that time, it entirely replaces and invalidates the preceding Equifax TaxCalc End User Terms and Conditions.

1.3. This Licence describes certain additional responsibilities and agreements that apply to Your use of the Anti-Money Laundering Identity Checking Service and the treatment of the data used in the AML Service, in addition to ASPL's Core Policies. It forms part of the T&Cs, EULA and CSA as per Section 1 of the T&Cs and runs concurrently with them.

1.4 Without prejudice of Section 1.5 below, material changes to the Service or to this ECL may be required as a result of:

1.4.1 the installation of any Equifax content such as software, update or improvements or ASPL's software, update or improvements; or
1.4.2 the application of any new laws, regulations acts or orders of the authorities, whereby the effect of the implementation is not known at the date of execution of the ECL.

1.5 ASPL shall be entitled at any time to improve, update or replace the Services in case of improvements or updates necessary to fix defects, bugs, malfunctioning or errors of the Service or to cure security vulnerabilities of the Service.

1.6 ASPL will provide notification of changes occurring under 1.4 and 1.5 via the TaxCalc Website and/or the Software.

1.7 Pursuant to this Licence, ASPL shall use reasonable efforts to ensure that the Anti-Money Laundering Identity Checking Service is available and operates in accordance with its intended specification, but ASPL does not guarantee, and excludes any warranty, condition or representation that Equifax will continue such a service. ASPL is not in any way responsible for any interference with or interruption to Your use of or access to the Anti-Money Laundering Identity Checking Service. ASPL may at any time change or discontinue any aspect of, availability or feature of its online functionality.

2 CORE POLICIES VARIATIONS

This clause clarifies the variations to the Core Policies in relation to this Licence:

Data Control, Identification and Sharing

2.1. You remain the Data Controller for personal data uploaded to the TaxCalc CloudConnect Service and any personal data therein is still your legal responsibility, as per Section 7 of our Privacy Policy.

2.2. You acknowledge and agree that:

2.2.1. In order to address endemic or specific issues in relation to the Product and/or Services provided by us, we may share administrative, sales and support data with Equifax. This may include personal data pertaining to You or Your clients.

2.2.2. Where You are suspected of being or actually in breach of our Core Policies or this Licence, we will notify Equifax of such a situation.

2.3. Equifax provides specific data to the Reseller ("**Output Data**") in response to Your search. Acorah utilises further data in the form of questions, including querying the level of risk, and the overall design. Combined with the Output Data, this forms the "**Mixed Data**" presented to the Customer. The data presented to the Customer may also contain data provided by the Customer directly.

Ordering & Payment

2.4. As a result of Your usage of the AML Service, You acknowledge and agree that Your order of the AML Service will be subject to acceptance and approval by Equifax. In the rare instance where there is an issue with this acceptance that cannot be resolved with reasonable endeavours (for example, applicability of the exceptions listed in Attachment 5), you will be entitled to contact ASPL for a

refund for Your Anti-Money Laundering Identity Checking purchase(s).

Provisioning & Liability

2.5 You acknowledge and agree that:

2.5.1 If we receive instruction from Equifax to cease provision of the AML Service to You, for any reason, we will cease provision of the AML Service to You.

2.5.2 The AML Service is intended to assist You in recording, assessing and reporting on processes and data in relation to Your Firm's compliance with money laundering regulations and due diligence checks. It does not and cannot verify the accuracy or correctness (including continued correctness) of the information entered by You and does not guarantee compliance to the relevant laws and regulations.

2.5.3 If an issue of a liability claim involving the AML Service arises, You should contact ASPL in the first instance.

2.5.4 To the maximum extent permitted by applicable law:

2.5.4.1 in no event shall ASPL or its suppliers be liable for any special, incidental, indirect or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the AML Service, the provision of or failure to provide support services, or otherwise under or in connection with any provision of this Licence, even in the event of the fault, tort (including negligence), strict liability, breach of contract, or breach of warranty of ASPL or any supplier, and even if ASPL or any supplier has been advised of the possibility of such damages; and

2.5.4.2 notwithstanding any damages that You might incur for any reason whatsoever (including, without limitation, all damages referred to above and all direct or general damages), the entire liability of ASPL and any of its suppliers under any provision of this Licence and Your exclusive remedy for all of the foregoing (except for any remedy of repair or replacement elected by ASPL with respect to any breach of ASPL's obligations) shall be limited to the amount actually paid by You for the AML Service in the preceding 12 month period. The foregoing limitations and exclusions shall apply to the maximum extent permitted by applicable law.

2.5.5 Equifax provides TaxCalc's Anti-Money Laundering Identity Checking Service that allows You to perform identity checks. ASPL does not guarantee:

2.5.5.1 that Equifax will continue such a service; and
2.5.5.2 the availability of the Equifax service.
2.5.5.3 ASPL is not in any way responsible for any interference with or interruption to Your use of or access to the Anti-Money Laundering Identity Checking Service. ASPL may at any time change or discontinue any aspect of, availability or feature of its online functionality.

3 REGARDING ATTACHMENTS TO THIS LICENCE

You agree to the following Attachments to this Licence:

3.1 The Customer Terms in Attachment 1;
3.2 The Dow Jones Data End User Terms in Attachment 2;
3.3 The External Party Baseline Security Standard in Attachment 3;
3.4 The Data Protection Policy in Attachment 4;
3.5 The Do Not Serve List in Attachment 5;
3.6 The Security Requirements Schedule in Attachment 6;
3.7 The Customer Application Form in Attachment 7.

ATTACHMENTS TO THE EQUIFAX LICENCE

ATTACHMENT 1: The Customer Terms

In consideration of the supply and use of the Information Services by you, the parties agree:

Definitions:

"**Agreement**" means the agreement between us and the Reseller under which we make available to the Reseller certain data services for resupply to end users;

"**Applicable Laws**" means all applicable laws, enactments, rules, regulations, orders, regulatory policies, regulatory permits and licences, and any mandatory instructions or requests of a regulator, in each case which are in force from time to time, including:

i. The Consumer Credit Acts 1974 and 2006;
ii. The Data Protection Act 2018;
iii. The Representation of the People (England and Wales) Regulations 2001;
iv. The Financial Services and Markets Act 2000 (Money Laundering Regulations 2001);
v. Rules made by the Steering Committee on Reciprocity; and
vi. The Guide to Credit Scoring 2000

"**Information Services**" means the services that you are authorised to receive via the Reseller that are provided to the Reseller under the Agreement;

"**Output Data**" means any information or data provided by Equifax as part of the Information Services;

"**Reseller**" means the third party through whom you are authorised to access the Information Services;

"**us**" and "**we**" means Equifax Limited; and

"**you**" has the meaning in the application form set out above these terms.

1. Confidentiality: use and non-disclosure of Output Data

1.1 You shall use the Output Data only as permitted by term 4 below or as otherwise permitted by the Reseller and shall not engage in any business involving the supply of any Output Data, or any information derived from any Output Data, to any other person.

1.2 Unless expressly permitted by the Reseller, you may not disclose to any other person any of the Output Data, except:

1.2.1 when required to do so by law or any regulatory authority; or

1.2.2 to your personnel whose duties reasonably require such disclosure, on condition that you ensure that each such person to whom such disclosure is made: (a) is informed of your obligation of non-disclosure and (b) complies with that obligations as if they were bound by it.

1.3 You shall maintain adequate security measures to protect the integrity, security and confidentiality of all Output Data (including complying with Equifax's security requirements and policies).

2. Applicable Laws

2.1 You shall comply at all times with the Applicable Laws.

2.2 You shall provide to us any information we may from time to time reasonably request in order for us to determine whether your use and possession of the Output Data is in compliance with the Applicable Laws.

2.3 We may cease to make the Output Data available to the Reseller for resupply to you if your response to any request we may make as contemplated by term 2.2 above does not satisfy us that your use and possession of the Output Data is in compliance with the Applicable Laws

2.4 The use of some types of the Output Data require you to be a member of the relevant "closed user group" and enter into, and comply with, any applicable closed user group agreements.

2.5 In utilising any Output Data, you are acting as a data controller and, as such must comply with all the obligations on a data controller imposed under the Data Protection Act 2018.

3. Notices

3.1 Before using any Information Services to obtain information relating to a natural person you shall notify the person that: (a) information which the person gives you may be disclosed to a credit reference agency, which may keep a record of that information; and (b) the credit reference agency may disclose that information, and the fact that a search was made, to its other customers for the purposes of assessing the risk of giving credit and occasionally to prevent fraud, money laundering and to trace debtors. You shall give the notification to the person in writing, unless doing so would unreasonably interfere with your activities. On our request you shall send us a copy, or transcript, of the notification you use.

3.2 To the extent that you are able to do so, you grant us a perpetual, royalty free right to record the

information referred to in term 3.1(a) for the purposes referred to in term 3.1(b).

3.3 The Reseller will notify you of the search type or types you are entitled to carry out when using the Information Services. We may from time to time change the search types which you are entitled to carry out. The Reseller will notify you in writing of any such changes in reasonable time before the change becomes effective. You shall ensure that you understand which search type code we require you to use for each kind of search you carry out using the Information Services and you shall ensure that you use the correct search type code at all times when using the Information Services.

4. Permitted Use

4.1 You shall not use the Output Data for any purpose other than: prevention of money laundering.

5. Limitation of liability

5.1 You acknowledge: (a) that most of the Output Data is provided to us by third parties which we do not control, in particular in relation to the accuracy or completeness of the Output Data; (b) that the volume and nature of the information on our databases makes it impractical for us to verify it; and (c) that, if we were to attempt to verify the Output Data, we would only be able to offer the Services to you at significantly increased cost. You agree that we shall not in any circumstances be liable for any loss or damage at all arising from any inaccuracies, faults or omissions in, or in the provision of, the Output Data unless caused by our negligence or wilful default.

5.2 You agree that we shall not in any circumstances (including without limitation if we have been negligent) be liable for (a) any indirect or consequential loss or damage at all; or (b) any loss of business, capital, profit, reputation or goodwill, arising out of or in connection with the Information Services or the Output Data.

5.3 Our entire liability in respect of any single cause of action arising out of or in connection with the Output Data or the Services (whether for breach of contract, negligence, under statute or otherwise) shall be limited to £50. You shall not be entitled to recover from us and the Reseller in respect of the same loss.

5.4 We shall not be liable for any claim arising under these terms unless you give us written notice of the claim within 3 months of becoming aware of the circumstances giving rise to the claim or, if earlier, 3 months from the time you ought reasonably to have become aware of such circumstances.

5.5 Nothing in these terms shall limit or exclude our liability for death, personal injury or fraud arising from our negligence.

5.6 Except as expressly provided in these terms, all representations, conditions and warranties whether express or implied (by statute or otherwise) are hereby excluded to the fullest extent permitted by law.

6. Audit

6.1 You shall allow Equifax and any advisers to Equifax to access on reasonable notice any of your premises, personnel and relevant records as may be reasonably required in order to undertake verification of your compliance with these Customer Terms.

6.2 You shall comply with your obligations as set out in any Applicable Laws, in relation to record keeping.

6.3 Subject to the obligations of confidentiality, you shall provide Equifax (and its advisers) all reasonable co-operation, access and assistance in relation to each audit.

6.4 If the audit identifies a default by you or there are reasonable grounds for Equifax to reasonably suspect a default, then without prejudice to any other rights or remedies available:

a) you shall take all necessary steps to comply with its obligations; and
b) Equifax may suspend the Information Services or terminate these terms immediately upon written notice.

7. General

7.1 Equifax may cease to supply those Information Services which relates to the provision of data if the data supply is no longer possible under any agreement Equifax has with third party suppliers. In such cases, the affected element of the Information Services shall terminate from the date on which Equifax can no longer perform the relevant Information Services.

7.2 These terms set out the entire agreement and understanding between you and us in connection with its subject matter. In particular, but without limitation to the generality of the foregoing, you warrant and represent that in entering into these terms you have not relied upon any statement of fact or opinion made by Equifax or our officers, servants or agents which has not been included expressly in these terms.

7.3 If any provision of these terms is or becomes invalid or unenforceable it will be severed from the rest of these terms so that it is ineffective to the extent that it is invalid or unenforceable and no other provision of these terms shall be rendered invalid, unenforceable or be otherwise affected.

7.4 In these terms: (a) the headings are inserted for convenience only and shall not affect their construction or interpretation; (b) unless the context requires otherwise, words importing the singular shall include the plural and vice versa; and (c) unless the context requires otherwise, references to any person include references to any human being, company, body corporate, association, joint venture, partnership, trust and any entity capable of suing and being sued.

7.5 These terms shall be governed by English law. The parties hereby submit to the exclusive jurisdiction of the English Courts.

ATTACHMENT 2: The Dow Jones Data End User Terms

The Customer shall when using the Equifax Watchlist abide by the following End User Agreement terms;

The terms set out in this End User Agreement (“**EUA**”) apply to the Dow Jones Data, which shall be considered as Data for the purpose of the agreement between the Customer and **Equifax Limited** (“**Equifax**”) (the “**Agreement**"). Unless otherwise defined in EUA, any defined terms shall have the meanings given in the Agreement.

In this EUA, the following terms shall have the following meanings:

"**Dow Jones Data**" means personal data (full name, maiden name or AKAs, place and date of birth, country of residence and country of citizenship, occupation and information on additional roles and the relationship (if applicable) to a public figure) compiled and maintained by Dow Jones on data subjects, including Politically Exposed Persons (PEPs) and Special Interest Persons (SIPs) which includes individuals due to his/her prominence in the news owing to his/her involvement in selected criminal activity:

"**Dow Jones**" means Factiva Limited, a company incorporated in England and Wales under number 3773253 and with registered address at The News Building, 1 London Bridge Street, SE1 9GF London, England, acting on behalf of Dow Jones & Company, Inc. and any of its affiliated companies; and

"**Permitted User**" **means** an individual authorised to access and use the Dow Jones Data and who is either: (a) an individual employee of the Customer; (b) an individual performing the functions of an employee on a temporary basis, independent contractor or consultant, in each case who is performing work for the Customer; or (c) an individual working for a company engaged by the Customer ("**Third Party Contractor**") to perform research using the Dow Jones Data on the Customer's behalf, for the benefit of the Customer] provided that the Customer: (i) assumes full responsibility and liability for the acts and omissions of all Permitted Users, as if such acts and omissions were committed or made by the Customer; and (ii) ensure that the Third Party Contractor and all Permitted Users use the passwords (provided by the Customer) only on a dedicated basis for the Customer.

1. Licence

1.1 Equifax will supply the Dow Jones Data to the Customer from the Start Date for the Dow Jones Data set out in the Customer Agreement and grants to the Customer a non-exclusive, non-transferable, non-sub licensable, non-assignable licence to use the Dow Jones Data subject to the terms and conditions of the Agreement and this EUA.
1.2 The Dow Jones Data contains information derived from publicly available sources, and will be regularly up-dated by **Equifax** as updates are received from Dow Jones. Dow Jones retains control and ownership of the form and content of the Dow Jones Data, and although Dow Jones may alter the Dow Jones Data from time to time, its fundamental nature will not be changed. The Customer and Permitted Users will not, under the Agreement and this EUA acquire any ownership rights in the Dow Jones Data.

2. Terms of use
2.1 The Customer and Permitted User shall use the Dow Jones Data in strict compliance with applicable laws and regulations within the jurisdictions in which it accesses and uses the Dow Jones Data. The Customer shall ensure that the Dow Jones Data shall only: (a) be accessed by Permitted Users; and (b) be used for the legitimate interests of the Customer and particularly for the purposes of assisting in complying with legal duties and regulations which apply to the Customer such as due diligence, anti-money laundering, "know your customer" compliance or similar regulatory screening obligations.
2.2 Except to the extent permitted or required for the Customer's permitted use under section 2.1, the Customer and/or Permitted Users shall not: (a) reproduce, distribute, display, sell, publish, broadcast or circulate the Dow Jones Data to any third party, nor make the Dow Jones Data available for any such use; or (b) create or store in electronic form any library or archive of the Dow Jones Data save that, and notwithstanding anything to the contrary, the Customer shall be entitled to

retain copies of the Dow Jones Data necessary for archival, regulatory and/or compliance purposes. The Customer's right to retain such copies as set forth above shall survive termination/expiration of this EUA provided that it no longer actively uses the Dow Jones Data.
2.3 The parties agree that upon termination of the provision of the Dow Jones Data and unless otherwise provided by subject applicable legal or regulatory restrictions, the Customer shall return or destroy all Dow Jones Data together with any copies, and certify in writing to **Equifax** the completion of this process. In the case where the Customer is required by law or regulation to keep copies of some of the Dow Jones Data, the Customer guarantees the confidentiality of the Dow Jones Data and will not use the Dow Jones Data for any other purpose.

3. Data Protection principles
3.1 The Customer shall comply with all applicable laws and regulations within the jurisdictions, in which the Customer processes the Dow Jones Data, and the Data Processing Principles set out below. The Customer acknowledges that an individual who is included in the Dow Jones Data (an "**Individual**") can enforce in his/her country of establishment this provision against the Customer with respect to its personal data. Any person acting under the authority of the Customer, including a data processor, shall be obligated to process the Dow Jones Data only on instructions from the Customer and on terms no less stringent than those set out in the Data Processing Principles below.
3.2 Upon reasonable request of **Equifax**, the Customer will submit its data processing facilities, data files and documentation needed for processing to review, audit and/or certification by **Equifax** (or any independent or impartial inspection agents or auditors, selected by **Equifax** and not unreasonably objected to by the Customer) to ascertain compliance with the warranties and undertakings in this EUA, with reasonable notice and during regular business hours. Such request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Customer, which consent or approval the Customer will attempt to obtain in a timely fashion.

4. Warranties

Equifax shall make reasonable efforts to ensure that the Dow Jones Data is up to date. While **Equifax** will use its reasonable efforts to ensure that the Dow Jones Data is complete, **Equifax** cannot warrant that the Dow Jones Data includes a complete or accurate archive of every public figure or their associates in each country. Except as specified in this EUA all express or implied representations, warranties, conditions and undertakings in relation to the provision of the Dow Jones Data are excluded.

5. Customer Information

Please note that **Equifax** will report to Dow Jones the name of the Customer and the number of name queries screened against the Dow Jones Data, but not its nature. This information will only be used by Dow Jones to verify the relevant usage of the Dow Jones Data and the payments due and payable to Dow Jones in this respect. Dow Jones shall not disclose such information to any third party, other than to members of its group companies, or use them for any other purpose whatsoever and will treat this information as Confidential Information.

Data Protection Principles

1. **Purpose limitation**: Personal Data may be processed and subsequently used or further

communicated only for the following purposes: (a) assisting in complying with legal duties and regulations which apply to the Customer Group; (b) performing a statutory role as a Governmental organization; or (c) performing law enforcement duties. If the Customer or a member of the Customer Group is processing special categories of data, defined under Article 8 of the European Directive 95/46/EC as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life ("Sensitive Data"), it shall only process it for the purpose of preventing fraud or a similar crime (the "Purposes").

2. **Personal Data quality and proportionality**: Personal Data must be accurate and, where necessary, kept up to date. Personal Data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. **Transparency**: Individuals must be provided with information necessary to ensure fair processing (such as information about the purposes for processing and about the transfer), unless such information has already been given by **Equifax**.

4. **Security and confidentiality**: Technical and organisational security measures must be taken by the Customer 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. This obligation shall not apply where the Customer is accessing services via the hosted solutions of **Equifax**.

5. **Rights of access, rectification, deletion and objection**: An Individual must, whether directly or via a third party, be provided with the Dow Jones Data about him/her that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or have been dismissed by the relevant data protection authorities, or when doing so would be likely to seriously harm the interests of the Customer or other organisations dealing with the Customer and such interests are not overridden by the interests for fundamental rights and freedoms of the Individual. The sources of the Dow Jones 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. An Individual must be able to have the Dow Jones Data about him/her 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, **Equifax** or the Customer may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the Dow Jones Data has been disclosed need not be made when this involves a disproportionate effort. The burden of proof for any refusal rests on the Customer or **Equifax**, and the Individual may always challenge a refusal before the relevant data protection authorities.

6. **Sensitive Data**: The Customer shall take such additional measures (e.g. relating to security) as are necessary to protect such Sensitive Data in accordance with its obligations under the Agreement or this EUA.

7. **Automated decisions**: For purposes hereof "automated decision" shall mean a decision by **Equifax** or the Customer which produces legal effects concerning an Individual or significantly affects an Individual and which is based solely on automated processing of Dow Jones Data intended to evaluate certain personal aspects relating to him/her, such as his/her performance at work, creditworthiness, reliability, conduct, etc. The Customer shall not make any automated decisions concerning Individuals, except when: (a) (i) such decisions are made by the Customer in entering into or performing a contract with the Individual, and (ii) the Individual 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 applicable laws or regulations.

ATTACHMENT 3: The External Party Baseline Security Standard

Reference to "**External Party**" within this Baseline Security Standard shall mean both the Reseller and the Customer.

1 Introduction

Equifax reserves the right to modify these Standards periodically with appropriate communication to External Parties which shall comply with this Standard as well as additional applicable and reasonable data security standards to which External Parties have agreed. This Standard is not intended to replace External Party's internal security policies, but rather provide requirements pertaining to the security of Equifax Sensitive Information and Equifax Information Resources.

2 Security Incidents and Investigations

External Party must notify Equifax as soon as possible, but within twenty-four (24) hours, following its awareness of a Security Incident which affects, or could affect, Equifax Data. All such notifications shall be made to the Equifax Security Incident Response Team (E-SIRT) at 1-888-257-8799 (+1-678-795-7106 from outside the US) or via email at security.incident@equifax.com. External Party shall perform the following tasks:

a. Take action to correct a suspected or confirmed Security Incident to the fullest extent reasonably practicable under the circumstances and include a description of that action, along with the report of the problem, to Equifax at the earliest possible time.

b. Monitor External Party Resources for Security Incidents and other suspicious activities; this includes suspicious external activity (including, but not limited to, unusual increase in network traffic, unauthorized probes, scans or break-in attempts) as well as suspicious internal activity (including, but not limited to, unusual increase in utilization/load, unauthorized system administrator access, unauthorized changes to External Party Resources or network, system or network misuse or Information Assets theft or mishandling).

c. Maintain, for a mutually agreed-upon length of time, all system records and logs related to Services, Agreement, and Access which Equifax may review and inspect with reasonable notice. External Party shall not be required to disclose to Equifax information that is External Party's confidential information not related to access and Services provided in the Agreement.

d. Provide any information that Equifax reasonably requests pertaining to the Security Incident and cooperate fully with Equifax to thoroughly investigate any such Security Incident.

2.1 Incident Response Plan

External Party shall document and implement a Security Incident response plan which all External Party Employees are required to follow in the event that a Security Incident is suspected or

confirmed; this Security Incident response plan shall include notifications, points of contact, backup procedures and all relevant actions that are required to recover from a Security Incident.

3 External Party Information Security Program Requirements

Protection of Information Resources and Sensitive Information requires, along with the other specific controls set forth in this Standard, the following preparedness and response activities:

a. Strict control over access (physical and logical) to, and use of, Information Assets, Sensitive Information and External Party Assets.

b. Upon Equifax's request, discontinuation or suspension of access to, and/or use of, Information Assets as well as securely returning or disposal of such hardware and/or software, including Sensitive Information and other information on Information Assets.

c. Protection against defacement, improper operation and/or loss of use of a System, including Information Resources, External Party Assets, application or website designed for, or in support of Equifax.

d. Protection of Information Assets, Sensitive Information and External Party Resources (on or off Equifax premises) including Information Resources and External Party Resources (e.g., an extranet connection) when using, operating or accessing the same.

3.1 General Security

a. External Party agrees to promptly implement and maintain an information security program that includes appropriate administrative, technical and physical safeguards reasonably designed to accomplish the following tasks:

i. Ensuring the security and confidentiality of Sensitive Information;

ii. Protection against damage, destruction and any anticipated potential threats or hazards to the security or integrity of such Sensitive Information;

iii. Safeguarding against unauthorized access to or use of such Sensitive Information that could result in substantial harm or inconvenience to any consumer; and

iv. Disposal of Sensitive Information in a secure manner.

b. External Party shall perform the following tasks:

i. Designating of an Employee or Employees to coordinate its information security program;

ii. Identification of internal and external risks to the security, confidentiality and integrity of Sensitive Information and Information Resources, and assessment of the sufficiency of any safeguards in place to control these risks.

iii. Design and implementation of information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures;

iv. Provision of access to Sensitive Information and Information Assets only to Employees with an

approved business need and perform regular entitlement reviews to ensure access is authorized and appropriate;

v. Encryption of all Sensitive Information during transmission or when at rest, including when stored on backup media. If External Party sends any Sensitive Information, the Sensitive Information must also be encrypted. Encryption methods must meet one of the following minimum encryption requirements:

• Advanced Encryption Standard (AES), minimum 128-bit key

• Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms

vii. Storing, using one-way hashing methods, of passwords on External Party Resources intended for Equifax usage and for systems containing Sensitive Information;

viii. Establishing a Key Management Process for protection of cryptographic keys;

ix. Retaining, using or storing Sensitive Information only as permitted under the Agreement;

x. At a minimum, annual completion of a security scan of the External Party Resources and correction of all significant vulnerabilities within a reasonable amount of time, based on the potential impact of the vulnerability. Summary results of this scan and any subsequent remediation will be shared with Equifax upon request;

xi. Implementation of security changes and patches in External Party Resources in a timely manner, as directed by the system manufacturer and subject to appropriate testing. Changes and patches must be implemented within ninety (90) days of their release. Security changes and patches correcting critical or immediate security risks must be implemented immediately, subject to appropriate testing as circumstances may allow, but no later than ten (10) days after their release unless a longer period is recommended by the manufacturer;

xii. Maintenance of individual access and accountability controls for each Employee who will access any Information Assets or Sensitive Information;

xiii. Provision and maintenance of secure authentication mechanisms for External Party Resources that cannot be bypassed to obtain access to the External Party Resources. One Time Password, smart cards or biometric devices are considered best practices. If passwords are to be used, they shall follow security best practices regarding the following:

- Length of password
- Complexities to include, but not be limited to, both alphabetic and numeric
- Password aging
- Password history
- Repeating characters
- Maximum invalid account login attempts
- Account lockout time limit
- Inactive session timeout

xv. Ensuring that all tokens given to Employees as part of two-factor authentication are unique to single users, and informing Employees that they are responsible for all activities performed with their token and that sharing of tokens is strictly forbidden;

xvi. Granting Remote Access, via approved two-factor authentication, only to Information Resources or Sensitive Information that an Employee has been approved to access;

xvii. Prohibiting of devices including, but not limited to, home personal computers (PCs)/laptops, personal mobile devices, personal email accounts, public PCs or PC kiosks to remotely access Information Resources via network connections such as VPN;

xviii. Configuration of devices to disable split tunneling. Split tunneling is defined as the ability to remotely connect to an internal corporate network (i.e., VPN) and connect to an external untrusted network simultaneously;

xix. Review of audit logs on devices allowing remote-access connectivity and/or mobile usage. Reviews shall be conducted at least once a month and logs shall be retained for a minimum of ninety (90) days online and one (1) year offline;

xx. Prohibiting of persistent connections to any Information Resource or any External Party Resources that contain, or have access to, Sensitive Information without permission by Equifax. Equifax has the right to refuse, disconnect or otherwise limit any persistent connection at any time, for any reason and without warning;

xxi. Protection of systems handling Sensitive Information with multiple layers of network security including, but not limited to firewalls, routers and intrusion detection/prevention devices (IDS/IPS).

3.2 External Party Facility

External Party shall have in place adequate physical and environmental security controls to maintain the confidentiality, availability and integrity of Information Assets and Sensitive Information including, but not limited to, the controls set forth below. External Party shall perform the following activities:

a. Securing of the perimeters of all External Party Facilities in which Sensitive Information will be accessed and/or stored. External Party Facilities shall be physically sound. The external walls of External Party Facilities shall be of solid construction and all external doors must be suitably protected against unauthorized access (e.g., control mechanisms, bars, alarms, locks, etc.).

b. Use of video surveillance to record access to External Party Facility and Secured Areas to deter intruders, protect Employees and be used as evidence in any civil or criminal proceedings. Recordings shall be retained for a minimum of thirty (30) days.

c. Securing of all doors with automatic closing devices such that all doors shall be secured at all times. All fire doors on a security perimeter shall be alarmed.

d. Restriction of access to External Party Facility to authorized personnel only; visitors must be logged and escorted at all times.

e. Locking of doors and windows when unattended. Additional external protection shall be provided for windows, particularly at ground level so as to not allow access or viewing of the interior of External Party Facility and/or where work is performed for Equifax.

f. Installation of suitable, monitored intruder detection systems, which shall be regularly tested. Systems must provide comprehensive surveillance of all external doors and windows and ensure that unoccupied areas are alarmed at all times.

g. Proper securing of system cabinets handling Sensitive Information when not in use for direct console access.

4 Information Handling and Destruction

Except as set forth herein or otherwise specified in the Agreement, External Party shall, in accordance with the requirements set forth below or in accordance with any timeframe specified by Equifax, destroy all Sensitive Information once it is no longer needed.

4.1 Shreddable Media

Paper, compact disks (CDs) and any other media that can be shredded; this media must be destroyed when External Party no longer needs the Information Resources contained thereon. This media may be destroyed immediately or temporarily stored in a secured, locked container. Media may be shredded at a location other than External Party's facilities, but it must be transferred in a secured, locked container with chain of custody documentation. External Party is responsible for the destruction regardless of where the activity occurs and by whom the destruction is performed. Information Resources present in this media must be completely destroyed such that the results are not readable or useable for any purpose.

5 Use of Subcontractors/Outsource Providers

The External Party must obtain written authorization from Equifax prior to subcontracting or offshoring all or any portion of the Services related to Information Assets or allowing any subcontractor or other third party provider to access Sensitive Information.

6 Non-Repudiation

6.1 Security Best Practices

External Party shall implement security best practices to ensure data integrity so that the repudiation of significant facts is negated by functionality involving a secure digital signature or another form of adequate proof that a certain person (and no other) performed a particular task.

a. Once an Employee has been authenticated as described above, External Party shall employ a verification scheme that identifies the Employee and provides an acceptable measure of security for access to Information Assets.

b. External Party must have procedures in place that create appropriate audit trails for all transactions and retain those audit trails for not less than ninety (90) days online and one (1) year offline.

c. External Party must take steps to protect Employee access by timing out the Employee session after a period of inactivity not to exceed fifteen (15) minutes.

7 External Party Employees Security

External Party must have a documented procedure to screen and board Employees before access is provided to any Information Assets or Sensitive Information, or to any External Party Assets providing access to such entities.

7.1 Employee Screening

External Party must have a documented pre-employment screening process that includes, but is not limited to, the following checks, as permitted by applicable law. Upon request from Equifax, External Party shall provide records and/or attestation of employee screening. Criminal History Screening: The review of criminal offenses on the individual's background record will include all localized law enforcement records for the past five (5) years (exclusive of any incarceration time).

7.2 Employee Boarding

Each External Party whose Employees have Access must complete the following procedures:

a. Conducting the appropriate level of employee screening on its Employees prior to Access being given. Only Employees that have passed the applicable screening requirements shall be provided Access.

b. Retaining of documentation which validates that the appropriate level of Employee screening requirements has been completed by the External Party and allowing Equifax to review such documentation upon request.

c. Maintenance and following of a written procedure for how the External Party will comply with the Employee screening and employee boarding requirements, which shall be available for review by Equifax upon request.

d. Requiring Employees to sign an acknowledgement of compliance with the External Party's security program.

If an Employee satisfies the employee screening requirements prior to being given Access, but External Party subsequently becomes aware of any information that would result in an Employee failing any of the requirements, External Party shall promptly remove the Employee's Access and prevent them from in accordance with the Agreement and these Standards. If any access device used by such providing Services or Accessing Sensitive Information or Information Resources Employee, such as Key Card or Remote Access token, cannot be recovered and returned to External Party, Equifax shall be immediately notified.

7.3 Security Awareness Program

External Party shall implement and maintain an ongoing security awareness program to educate Employees regarding security issues and the requirements of this document. The program must include, but should not be limited to, education regarding the following:

a. Email usage

b. Password management

c. Social Engineering, including phishing

d. Mobile device usage

e. Use of social media during job hours

f. How to contact management to report a security concern

External Party shall ensure that Employees are recertified annually and shall maintain documentation of Employee’s current training.

8 External Party Resources

In each instance where an External Party Resource is used to access Information Resources or Sensitive Information, the External Party Resource must be currently supported by the applicable system vendor(s). Critical operating system, application software and security patches, as determined by the software vendor, shall be applied to the device in a timely manner.

Removable devices or media such as, but not limited to mobile devices, Universal Serial Bus (USB) drives, magnetic tapes, digital video disks (DVDs) and CDs are not allowed to connect to any Information Asset or External Party Resource where Sensitive Information is held or processed. All methods of removable storage shall be blocked.

8.1 Anti-Virus and Protections against Malware and Malicious Code

External Party shall keep Information Assets, External Party Resources and Sensitive Information free of known viruses and other exploitive or destructive computer code. External Party shall adhere to the following requirements:

a. External Party shall use a regularly updated and current virus scanning software product in an active monitoring mode when using External Party Assets.

b. Where computing devices owned by the External Party are used for access to an Information Resources, the External Party shall ensure that critical operating system and application software security patches, as determined by the software vendor, are applied to the device in a timely manner.

c. Any applications developed by the External Party used for access to an Information Asset or Sensitive Information must follow the terms of the Agreement and a documented Software Development Life Cycle (SDLC) and include application security testing.

9 Business Continuity and Disaster Recovery

The External Party shall have a current documented Business Continuity Plan (BCP). Equifax reserves the right to audit the items included in the BCP. The BCP shall include, at a minimum, the following information:

a. Critical functions identified

b. Critical resources identified including, but not limited to, Employees, hardware, software and documentation

c. Strategy for critical functions and steps for restoration for all functions impacting Equifax

d. Call lists for employees, suppliers and customers

e. Service levels as they pertain to business functions

f. Workarounds where necessary

g. Dependency on any critical Information Technology (IT) functions, as referenced by a specific Disaster Recovery Plan (see Disaster Recovery subsection below)

External Party shall ensure that there is a person appointed by External Party and charged with the responsibility of developing and maintaining the BCP. The BCP shall be updated and tested at least annually. Current test results of BCP testing shall be retained until the next testing occurrence has been completed.

9.1 Disaster Recovery

The External Party shall have documented disaster recovery plans, provisioning and tested disaster recovery capabilities in place which can recover within an acceptable amount of time those critical business functions/Services for which Equifax has contracted, and restore connectivity from the External Party's recovery site to Equifax.

In keeping with industry standards and best practices, External Party plans shall be reviewed and successfully tested at a minimum annually.

External Parties shall make available, upon written request, the most current test report for systems or critical business processes utilized in support of Equifax with summary of corrective actions accomplished for any identified substantive plan or provisioning shortfalls discovered in the testing process.

9.2 Information Back-Up

Unless mutually agreed, External Party shall backup Information Assets and Sensitive Information in a periodic and timely manner. Backup copies must be labeled, logged and an up-to- date inventory kept.

10 PCI Data Security

Payment Card Industry (PCI) Data is comprised of cardholder account numbers, security codes and personal identification (PIN) numbers and any other categories of data subsequently identified by PCI Security Standards Council (SSC) as being subject to its Data Security Standards, which are currently published at the following URL: https://www.pcisecuritystandards.org. If External Party receives PCI Data from Equifax, External Party represents and warrants that it has in place, and shall maintain in place for as long as it has possession of and/or access to PCI Data, a compliant system for transmission, reception, storage and use of such PCI Data. In addition, External Party represents and warrants that it can now and shall continue to be able to evidence that it has been deemed PCI Compliant by PCI and shall maintain such designation during the time period External Party has possession of and/or access to PCI Data. External Party will provide annual attestation that it is compliant with current Payment Card Industry Data Standard.

Additionally, in the event of an actual or suspected Security Incident regarding PCI Data, External Party shall immediately notify Equifax and cooperate with the investigative actions of VISA, MasterCard, American Express, Discover Financial Services, JCB International, its representatives, other card providers, Equifax and/or its affiliates, or any appropriate law enforcement entity.

11 Assessment of Adherence to Security Standard

a. Subject to clause 15, at its own expense, Equifax may periodically conduct an audit, test or inspection (or collectively, "Assessment") of External Party to determine External Party's compliance with this Standard and the Agreement. External Party will cooperate in all such assessments, which may be required prior to the initiation of any Services. Equifax (or a third party designated by Equifax) may conduct onsite Assessments at each External Party Facility where work is performed, during normal business hours, upon reasonable notice and subject to reasonable confidentiality obligations. In the event that Equifax has a reasonable suspicion that External Party is not in compliance with this or any applicable Standard or Policy, Equifax may conduct additional assessments.

b. Such assessments shall be conducted on a mutually agreed upon date which shall be no more than ten (10) business days after Equifax's written notice of time, location and duration, subject to reasonable postponement by External Party upon External Party's request, provided that such postponement does not exceed twenty (20) business days and that no such postponement shall apply in the case of a Security Incident.

c. Following an assessment, Equifax will provide to External Party a copy of the summary report of findings and applicable recommendations for remediating these observations, along with appropriate remediation timelines based on the identified risk criticality. External Party shall be required to remediate, at its own expense, any Observations of the Assessment. If External Party fails to remediate any observations and provide supporting evidence of such remediation, Equifax shall be entitled, at External Party's expense, to perform additional assessments within that year in order to confirm (or refute) any claims of remediation. External Party agrees to promptly take action at its expense to address and correct any outstanding observations.

d. Equifax and its auditors will maintain the confidentiality of External Party's procedures and processes disclosed as a result of the Assessment which External Party describes as confidential.

e. External Party agrees that any failure to cooperate fully and promptly with the conducting of any Assessment requested pursuant to this section will be considered a material breach of the Agreement and constitute grounds for Equifax to immediately prohibit the provision of Sensitive Information and/or access to Information Assets to External Party.

ATTACHMENT 4: The Data Protection Policy

1. Transferred Data

1.1 Each Party may supply, licence or otherwise make available data to the other party pursuant to the terms of this Agreement and any Statement of Work. Such data shall be processed in accordance with the terms of this Agreement.

1.2 The Parties acknowledge that they are separate and independent data controllers.

1.3 The Parties shall each comply with their respective obligations under the Data Protection Laws when processing personal data.

1.4 In respect of data supplied by the Customer to the Reseller and the Reseller to Equifax and Searches:

1.4.1 the Reseller shall ensure that each Customer adopts CRAIN into its terms of business or otherwise provide an appropriate written notification to data subjects setting out that:

(a) the information which the individual gives to the Customer, is given to the Reseller, and the Reseller may disclose it to a credit reference or fraud prevention agency which may keep a record of that information; and

(b) the credit reference or fraud prevention agency may disclose that information, and the fact that a Search was made, to its other customers for the purposes of verifying identity, assessing the risk of giving credit, preventing fraud and tracing debtors;

1.4.2 the Reseller shall, at Equifax's request, give Equifax a copy of the notification the Customer uses for the purposes of complying with paragraph 1.4.1; and

1.4.3 the Reseller grants to Equifax a perpetual, royalty free right to keep a record of the information referred to in paragraph 1.4.1 for the purposes set out therein.

1.5 The Reseller must ensure Customers use the correct Search type codes when using the Information Services to make a Search to ensure that the resulting Footprint is accurate and reflects the Search undertaken. To do otherwise may distort and create an inaccurate credit report for an individual/company and affects the identity of the persons to whom the data is visible.

1.6 Equifax shall provide the Reseller with the Search type or types and types codes, which Equifax may change from time to time on reasonable notice and the Reseller shall ensure they are provided to the Customer.

1.7 Any failure to use the correct Search codes will be a material breach permitting Equifax to terminate this Agreement.

1.8 In respect of data supplied by Equifax to the Reseller for onward supply to the Customer:

1.8.1 data is supplied for the Reseller’s and Customer’s own internal purposes only; and

1.8.2 each Statement of Work sets out a description of the data, the specific permitted use and restrictions applying to the data, and any additional terms required to be passed through to the Reseller and the Customer.

2. Warranties

2.1 Each party has represented prior to the date of this Agreement, and warrants and covenants during the term of this Agreement that, in respect of the data it transfers to the other under this Agreement:

2.1.1 it has been obtained in accordance with the Data Protection Laws; and

2.1.2 its transfer to the other party in accordance with this Agreement will not constitute a breach of the Data Protection Laws.

2.2 Each party warrants and covenants during the term of this Agreement that following transfer to it, it shall process data in accordance with the Data Protection Laws.

2.3 The parties acknowledge and agree that the fact that any provision is expressed as a warranty shall not preclude any right of termination a party may have in respect a breach of that provision by the other party.

3. Security

3.1 Each party shall implement appropriate technical and organisational measures to ensure a level of Security appropriate to the risk involved under this Agreement to:

3.1.1 protect all data from unauthorised use, alteration, access or disclosure, and loss, theft, and damage, and to protect and ensure the confidentiality, integrity and availability of data; and

3.1.2 prevent a breach of security.

3.2 The Reseller shall comply and shall procure the Customer complies with the Equifax Security Requirements Schedule including the External Party Baseline Security Standard. If there is any conflict or inconsistency between the Equifax Security Requirements and the remainder of this Agreement, the Equifax Security Requirements and External Party Baseline Security Standard shall prevail to the extent of such conflict or inconsistency.

3.3 Each party shall keep accurate records of the security measures which it has in place and shall make such records available to the other upon request.

3.4 Security measures shall be regularly tested by each party to assess the effectiveness of the measures in ensuring the security, confidentiality, integrity, availability and resilience of data, and each party's compliance with this Agreement and each party's obligations under the Data Protection Laws. Each party shall maintain records of the testing.

3.5 In the event of a breach of security, the party subject to the breach shall notify the other party without undue delay.

3.6 Following the notification referred to in paragraph 3.5 above each party shall provide assistance and co-operation with the other party to mitigate the breach of security, at the cost of the party subject to the breach of security, including to take all necessary actions to prevent, contain, and mitigate the impact of such breach.

4. Records, notification and assistance

4.1 Each party shall at its own cost:

4.1.1 keep a record of any processing of data it carries out;

4.1.2 notify the other party promptly should it:

(b) receive any communication from a data subject whose personal data forms part of the Output Data seeking to exercise rights conferred on the data subject by the Data Protection Laws, or in respect of any complaint by a data subject or any complaint or any information notices, enforcement notice or other material correspondence from a Supervisory Authority (including the FCA), in respect of data transferred under this Agreement; or

(a) become aware of any circumstance which may cause either party to breach this Agreement or which may cause either party to breach the Data Protection Laws; and

4.1.3 reasonably cooperate and coordinate with the other party and any Supervisory Authority (including the FCA) concerning the other party's compliance with Data Protection Laws.

ATTACHMENT 5: The Do Not Serve List

The following business purposes cannot be provided with Equifax data of any kind (including employment services) for any purpose:

- Adult entertainment services of any kind
- Companies that handle physical third party repossession
- Companies that locate missing children
- Dating services
- Massage services
- Tattoo services
- Companies that charge advance fees for debt or mortgage assistance relief (excluding refinancing of a dwelling loan or services offered by attorneys)
- Private investigation or detective services (excluding assisting with pre-employment services with written consent)

ATTACHMENT 6: The Equifax Security Requirement Schedule

1. These Security Requirements apply to any means through which the Customer orders or accesses the Services including, without limitation, system-to-system, direct access terminal, personal computer or the Internet.

2. These requirements of this Schedule are in addition to any requirements imposed by Applicable Law which apply to the Customer’s use of the Services.

3. For the purposes of these Security Requirements "Authorised User" means a Customer or an employee that the Customer has authorised to order or access the Services and who is aware of and trained in the Customer’s obligations under the terms of this Agreement with respect to the access to and use of the Services.

4. The Customer will:

4.1 ensure that only Authorised Users can order or have access to the Services;
4.2 ensure that Authorised Users do not order credit reports for personal reasons or provide

them to any third party unless expressly permitted by any agreement by the Reseller and Equifax;

4.4 take all necessary measures to prevent unauthorised ordering of or access to the Services by any person other than an Authorised User for permissible purposes, including, without limitation; limiting the knowledge of the Customer's security codes, any telephone access number(s) Equifax provides, and any passwords the Customer may use, to those individuals with a need to know; changing the Customer's user passwords at least every ninety (90) days, or sooner if an Authorised User is no longer responsible for accessing the Information Services, or if the Customer suspects an unauthorised person has learned the password; and using all security features in the software and hardware the Customer uses to order or access the Services;

4.5 not use personal computer hard drives or portable or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs, DVDs, software, and code) to store the Services. In addition, Output Data must be encrypted when not in use and all printed Output Data must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed, by the use of cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose;

4.7 monitor compliance with the obligations of these Security Requirements, and without undue delay notify Equifax if the Customer suspects or knows of any unauthorised access or attempt to access the Information Services. To assist compliance with this paragraph 4.7 the Customer shall create a process to report any suspicious or unauthorised activities or access immediately upon them becoming aware of the same;

4.8 not ship hardware or software between the Customer's locations or to third parties without deleting number(s), security codes, telephone access number(s) and passwords relevant to Equifax;

4.9 use best endeavours to assure Output Data security when disposing of any consumer report information or record obtained from Equifax.

5. The Reseller or Equifax may suspend the Services and the supply of Output Data if, acting reasonably, the Reseller or Equifax believes the Customer has suffered, is suffering, or may suffer a breach or attempt to breach its security.

6. During any period of suspension:

6.1 the Customer will cooperate with the Reseller and Equifax to address the cause of any concerns; and

6.2 neither Equifax nor the Customer will issue any public statement regarding the Services or the Output Data and identifying the other party, unless required to do so by Applicable Law.

7. Equifax will reinstate any suspended services as soon as it is satisfied as to the security of the Services and the Output Data.

8. The Customer will comply with the Customer Licence, including with these Security Requirements and Equifax's External Party Baseline Security Standard (Attachment 3), as amended from time to time.

ATTACHMENT 7: The Customer Application Form

Equifax Limited ("**Equifax"**) and Acorah Software Products Limited t/a TaxCalc ("**Reseller"**) are parties to the Agreement under which Equifax makes available to the Reseller certain data services for resupply to end users ("**End User**"). Equifax may be willing to permit You to become an End User.

Equifax reserves the right at its sole discretion to decide whether to accept or reject your request to become an End User. If Equifax does accept you as an End User it shall be under such conditions as Equifax specifies (which shall include, but not be limited to, Your compliance with the provisions of the Customer Licence). If Equifax does accept you as an End User, Equifax or the Reseller shall notify You of such in writing and the Customer Licence shall duly apply.

In addition, Equifax reserves the right to request the following information from You at any time: Your name as client/requestor; Your trading name; Your Companies House Registration Number; Your registered address; Your Data Protection Registration Number; Your industry sector; and Your explanation of the circumstances upon which You will carry out searches.