Services Agreement

This Agreement is made between:

(1) TransUnion International UK Limited (registered in England and Wales with company number 03961870) the registered office of which is at One Park Lane, Leeds, West Yorkshire, LS3 1EP ("**TransUnion**"); and

(2) [CLIENT] (registered in England and Wales with company number [ ]) the registered office of which is at [ ] (the "**Client**").

The Client wishes TransUnion to provide certain services to the Client and TransUnion wishes to provide such services. This Agreement sets out the parties' understanding as to the terms on which such services shall be provided. By signing this front page the parties agree to be bound by the terms of this Agreement.

This Agreement comprises:

- this front page;
- Primary Schedule;
- Service Schedule ([insert relevant Service(s) being taken]);
- Payment Schedule;
- and the General Terms attached to it.

This Agreement shall be interpreted subject to (to the extent of any inconsistency, in descending order of precedence) any relevant Service Conditions contained within a Service Schedule, the Primary Schedule, the General Terms, any Notes in the Payment Schedule and any other part of the Schedules.

Signed for and on behalf of TransUnion International UK Limited	Signed for and on behalf of [CLIENT]
……………………………………………… Signature	……………………………………………… Signature
……………………………………………… Name of authorised signatory	……………………………………………… Name of authorised signatory
……………………………………………… Position	……………………………………………… Position
……………………………………………… Date	……………………………………………… Date

For TransUnion use only:
Version: 082

PRIMARY SCHEDULE

TRANSUNION INFORMATION

Full Name:	TransUnion International UK Limited
Company Number:	03961870
Registered Office Address:	One Park Lane, Leeds, West Yorkshire, LS3 1EP
Telephone Number:	0113 538 0016
E-Mail:	UKClientServiceDesk@transunion.com (for support and queries)

CLIENT INFORMATION

Full Client Name:	[ ]
Company Number:	[ ]
Registered Office Address:	[ ]
Telephone Number:	[ ]
E-Mail:	[ ]

CLOSED USER GROUP DATA

1. For the purpose of the following paragraphs, the following additional definitions apply:
   "**Closed User Group**" means a closed user group database comprising data provided to TransUnion by Members which is compiled and hosted by TransUnion on behalf of Members.
   "**Closed User Group Data**" means data from a Closed User Group.
   "**Closed User Group Rules**" the rules of the relevant Closed User Group (as updated from time to time), copies of which shall be made available by TransUnion upon request.
   "**Member**" means a party that TransUnion has admitted as a member of the relevant Closed User Group.
2. Notwithstanding anything to the contrary in this Agreement, access to Closed User Group Data shall only be available to Members who are making appropriate contributions to the relevant Closed User Group or are otherwise entitled to access such data in accordance with the relevant Closed User Group Rules ("**Closed User Group Access Requirements**"). The Client shall observe the relevant Closed User Group Rules when utilising Closed User Group Data.
3. To the extent the Client is accessing Closed User Group Data and subsequently is no longer entitled to access such data, TransUnion, acting reasonably and without prejudice to its other remedies, shall have the right to:
   3.1 adjust the level of Closed User Group Data returned in the Services, in compliance with the relevant Closed User Group Rules; or
   3.2 where 3.1 is not practicable, suspend and/or terminate (as the case may be) the relevant Services, by giving written notice to the Client.
4. Where suspension and/or termination of the Services results from the Client's cessation of appropriate contributions to the relevant Closed User Group, such suspension and/or termination shall not affect the Client's obligation to pay the relevant fees for those Services, which shall continue in full force and effect.

5. **SHARE**
   5.1 For the purpose of the following paragraphs, the following additional definitions apply:
   "**Consumer Account Performance Data**" means data derived from the Member's operation of its consumer credit accounts.
   "**Credit Data Industry Regulator**" means the entity that regulates the use and sharing of credit performance data in the UK, presently the Steering Committee on Reciprocity ("**SCOR**") which is an unincorporated committee.
   "**Principles of Reciprocity**" means the Closed User Group Rules established by the Credit Data Industry Regulator which govern the use of shared data in the credit industry, presently available at https://www.scoronline.co.uk/.
   "**SHARE**" means the Closed User Group comprising Consumer Account Performance Data.
   5.2 The Client acknowledges that the use of SHARE data is governed by the Principles of Reciprocity.
   5.3 Without prejudice to any other term of this Agreement, the Client shall ensure that within the constraints of the Permitted Purpose, the category(ies) of SHARE data accessed by the Client as part of the Services and the Output are used by the Client strictly in accordance with the "**Decision Type & Data Availability**" matrices contained in section 2 of the Principles of Reciprocity (as updated or replaced from time to time with provisions having the same purpose).

FREEDOM OF INFORMATION

These additional Service Conditions shall apply when the Client is (or is acting on behalf of) a Public Authority (as defined below).

1. In respect of these Service Conditions, the following additional definitions apply:
   "**EIR**" means the Environmental Information Regulations 2004 and/or the Environmental Information (Scotland) Regulations 2004 (as applicable);
   "**FoIA**" means the Freedom of Information Act 2000 and/or the Freedom of Information (Scotland) Act 2002 (as applicable);
   "**Public Authority**" means (i) a public authority or a Scottish public authority as defined in section 3 of FoIA; or (ii) any other organisation otherwise subject to the requirements of FoIA or EIR.

2. If the Client receives a request for information under FoIA or EIR which relates to the subject matter of this Agreement, including any of the Confidential Information or Output disclosed to the Client, the Client shall (and shall ensure that any agent or sub-contractor of the Client shall) use all reasonable endeavours to:
   2.1 inform TransUnion that the request has been received and provide TransUnion with full details of the request as soon as practicable and in any event within three working days of its receipt; and
   2.2 consult with TransUnion before any information is disclosed in response to the request, which shall include consultation as to the application of any exemptions to disclosure under FoIA or EIR and as to the content of any information to be disclosed.

DURATION

Unless otherwise agreed in respect of a particular Service Schedule, the duration of this Agreement for the purposes of clause 2 of the General Terms shall be set out in the G-Cloud Call Off Contract.

SERVICE SCHEDULE
CALLVALIDATE INTERNATIONAL (ONLINE & BATCH)
CALLVALIDATE UK (ONLINE & BATCH)

Commented [MS1]: This Service Schedule contains all options - the Schedule will need to be tailored to reflect the particular options and permitted purposes applicable for the relevant client at Call-Off stage. Therefore, not all provisions in this Service Schedule will be applicable at the Call-Off stage.

1. **DESCRIPTION OF THE SERVICES**

In this Service Schedule, the Services shall comprise the following:

Online Service(s):

1.1 CallValidate International, comprising:
- Verification

1.2 CallValidate UK, comprising:
- CallML
- CallML Value Added Service: Deceased Check
- CallML Value Added Service: CIFAS
- CallML Value Added Service: Alternate Address Link
- CallML Value Added Service: Watchlist Screening
- CallML Value Added Service: Age Verification
- CallML Value Added Service: Activity History
- CallID (Employment Check)
- CallID Enhanced
- CallID Value Added Service: Deceased Check
- CallID Value Added Service: CIFAS
- CallID Value Added Service: Alternate Address Link
- CallID Value Added Service: Age Verification
- CallID Value Added Service: Activity History
- Bank
- Card
- Card Live
- Delivery Fraud Check
- Real Time Fraud Alerts
- Ownership Fraud Alert (Bank)
- Ownership Fraud Alert (Card)
- CallValidate3D
- Bank Account Premium
- NCOA® Alert
- EmailID
- MobileID
- EmailRisk
- DeviceRisk including:
    - SureScore
    - Advanced Transaction Model
    - IP Reputation Lite
- MobileRisk Standard/MobileRisk Live/MobileRisk Score ("**MobileRisk**")
- MobileKYC
- MobileSimSwap
- MobileRedirect
- CardID
- BankAccountID
- CallValidate Scorecard
- Age Verification Standard

1.3 Web Access

1.4 Set up and maintenance of (i) a standalone API; and (ii) the TransUnion Cosmos™ API, for delivery of the Online Service

1.5 The provision of software (including, where appropriate, a software development kit) designed to collect certain device technical data and user interaction attributes (the "**Device Identifying Software**"), which must be installed on the Client's website and/or mobile application

1.6 Access to the Intelligence Center

1.7 Set-up and delivery of EmailRisk/MobileRisk via the CallValidate UK vault, which is a data storage facility that allows the Client to access and download certain information on searches they have previously processed through CallValidate UK (the "**Vault**")

1.8 EmailRisk/MobileRisk Output from the Vault which can, at the Client's option, be manually accessed through the CallValidate UK web interface or set to automatically download to the Client's SFTP folder on a daily, weekly or monthly basis

Batch Service(s):

1.9 CallValidate International, comprising:
- Verification

1.9.1 One-off batch processing ServiceOngoing batch processing Service

1.10 **CallValidate International Input**

1.10.1 The Client shall provide TransUnion with one file comprising up to [INSERT VOLUME] customer records on a date to be agreed between the parties.

1.10.2 The Client shall provide TransUnion with a maximum of [INSERT VOLUME] customer records [INSERT FREQUENCY OF BATCH SUBMISSIONS]. Each file submitted by the Client shall comprise not less than [INSERT MINIMUM VOLUME PER FILE] customer records per file. The dates on which such files shall be provided to TransUnion shall be agreed between the parties from time to time.

1.10.3 The Client shall provide TransUnion with the Input files comprising up to the following customer records:

Input File Reference:	Volume of Customer Records:
Input File 1	[INSERT VOLUME]
Input File 2	[INSERT VOLUME]
Input File 3	[INSERT VOLUME]

Input File 4	[INSERT VOLUME]
Input File 5	[INSERT VOLUME]
Input File 6	[INSERT VOLUME]
Input File 7	[INSERT VOLUME]
Input File 8	[INSERT VOLUME]
Input File 9	[INSERT VOLUME]
Input File 10	[INSERT VOLUME]

Such files shall be provided to TransUnion on dates to be agreed between the parties.

1.10.4 The Client shall provide TransUnion with [INSERT OTHER DETAILS] customer records during each Year of this Agreement. The dates on which such files shall be provided to TransUnion shall be agreed between the parties from time to time.

1.10.5 [INSERT INPUT STATEMENT].

1.11 **CallValidate International Output**

1.11.1 The CallValidate International Service shall comprise batch processing of the Input [INSERT HOW MANY TIMES FILE IS BEING PROCESSED] against appropriate international databases, resulting in the Output comprising the Input appended with the following variable (where available):

- ID Check

1.12 CallValidate UK, comprising:

- CallML
- CallML Value Added Service: Deceased Check
- CallML Value Added Service: CIFAS
- CallML Value Added Service: Alternate Address Link
- CallML Value Added Service: Watchlist Screening
- CallML Value Added Service: Age Verification
- CallML Value Added Service: Activity History
- CallID (Employment Check)
- CallID Enhanced
- CallID Value Added Service: Age Verification
- CallID Value Added Service: Deceased Check
- CallID Value Added Service: CIFAS
- CallID Value Added Service: Alternate Address Link
- CallID Value Added Service: Activity History
- Bank
- Card
- Card Live
- Delivery Fraud Check
- Real Time Fraud Alerts
- Ownership Fraud Alert (Bank)
- Ownership Fraud Alert (Card)
- CallValidate3D
- Bank Account Premium
- NCOA® Alert
- EmailID
- MobileID
- BankAccountID
- CardID
- EmailRisk
- MobileRisk Standard/MobileRisk Live/MobileRisk Score (“**MobileRisk**”)
- MobileKYC
- MobileSimSwap
- MobileRedirect
- Age Verification Standard

1.12.1 One-off batch processing ServiceOngoing batch processing ServiceProof of concept

1.13 **CallValidate UK Input**

1.13.1 The Client shall provide TransUnion with one file comprising up to [INSERT VOLUME] customer records on a date to be agreed between the parties.

1.13.2 The Client shall provide TransUnion with a maximum of [INSERT VOLUME] customer records [INSERT FREQUENCY OF BATCH SUBMISSIONS]. Each file submitted by the Client shall comprise not less than [INSERT MINIMUM VOLUME PER FILE] customer records per file. The dates on which such files shall be provided to TransUnion shall be agreed between the parties from time to time.

1.13.3 The Client shall provide TransUnion with the Input files comprising up to the following customer records:

Input File Reference:	Volume of Customer Records:
Input File 1	[INSERT VOLUME]
Input File 2	[INSERT VOLUME]
Input File 3	[INSERT VOLUME]
Input File 4	[INSERT VOLUME]
Input File 5	[INSERT VOLUME]
Input File 6	[INSERT VOLUME]
Input File 7	[INSERT VOLUME]
Input File 8	[INSERT VOLUME]
Input File 9	[INSERT VOLUME]
Input File 10	[INSERT VOLUME]

Such files shall be provided to TransUnion on dates to be agreed between the parties.

1.13.4 The Client shall provide TransUnion with [INSERT OTHER DETAILS] customer records during each Year of this Agreement. The dates on which such files shall be provided to TransUnion shall be agreed between the parties from time to time.

1.13.5 [INSERT INPUT STATEMENT].

1.14 **CallValidate UK Output**

1.14.1 The CallValidate UK Service shall comprise batch processing of the Input [INSERT HOW MANY TIMES FILE IS BEING PROCESSED] against appropriate UK databases, resulting in the Output comprising the Input appended with the variables as set out in paragraph 1.12 above. In respect of CallValidate3D element only, a report shall be provided summarising the Input as appended.

1.14.2 In addition to the above, TransUnion shall provide the Client with a report based on a retrospective analysis of the Output undertaken by TransUnion, to provide key insights into how such CallValidate UK elements would have performed in a live production environment in respect of those customer records contained within the Input (**'Report'**).

2. **PERMITTED PURPOSE**

ONLINE SERVICES:

2.1 **CallValidate International:**

To verify the identity of individuals or to provide address and residency confirmation for the Client's internal business purposes only.

2.2 **CallValidate UK:**

(1) To make internal business decisions in respect of anti-money laundering to support an inbound financial transaction relationship, for the Client's internal business purposes only; and (2) To verify that particular sort codes, account numbers and credit/debit card numbers are valid to aid in the identification and prevention of high fraud risks, for the Client's internal business purposes only.

2.3 **CallValidate UK:**

(1) To make internal business decisions in respect of identity verification to support an inbound financial transaction relationship, but only where the financial transaction is the giving of credit or an application that may result in the giving of credit or the giving of any guarantee, indemnity or assurance in relation to the giving of credit, for the Client's internal business purposes only; and (2) To verify that particular sort codes, account numbers and credit/debit card numbers are valid to aid in the identification and prevention of high fraud risks, for the Client's internal business purposes only.

2.4 **CallValidate UK:**

(1) To make internal business decisions in respect of anti-money laundering and or identity verification (as applicable) to support an inbound financial transaction relationship, for the Client's internal business purposes only (when used for identity verification purposes, only where the financial transaction is the giving of credit or an application that may result in the giving of credit or the giving of any guarantee, indemnity or assurance in relation to the giving of credit); and (2) To verify that particular sort codes, account numbers and credit/debit card numbers are valid to aid in the identification and prevention of high fraud risks, for the Client's internal business purposes only (as applicable).

2.5 **CallValidate UK:**

To make internal business decisions in respect of identity verification, when pre-checking an individual for the suitability of employment or as part of an ongoing employment check, for the Client's internal business purposes only.

2.6 **CallValidate UK:**

To make internal business decisions in respect of age verification to support an inbound financial transaction relationship, for the Client's internal business purposes only.

2.7 **Watchlist Screening:**

To assist the Client in performing customer or counterparty due diligence and other screening and risk management activities carried out to support an inbound financial transaction relationship and to comply with legal or regulatory obligations to which the Client is subject, in particular in relation the ML Regulations, Sanctions Legislation or any rules made pursuant to section 137A of the Financial Services and Markets Act 2000, for the Client's internal business purposes only.

2.8 **EmailID:**

To assist the Client in assessing associations between an individual's identity and a given email address to support identity verification, fraud prevention and/or anti-money laundering processes, for the Client's internal business purposes only.

2.9 **MobileID:**

To assist the Client in assessing associations between an individual's identity and a given telephone number to support identity verification, fraud prevention and/or anti-money laundering processes, for the Client's internal business purposes only.

2.10 **BankAccountID:**

To assist the Client in assessing associations between an individual's identity and a given bank account number/sort code to support identity verification, fraud prevention and/or anti-money laundering processes, for the Client's internal business purposes only.

2.11 **CardID:**

To assist the Client in assessing associations between an individual's identity and a given card number to support identity verification, fraud prevention and/or anti-money laundering processes, for the Client's internal business purposes only.

2.12 **DeviceRisk:**

To identify suspicious and/or high risk devices used by individual users that access the Client's website and/or mobile application, for the Client's internal business purposes only.

2.13 **EmailRisk:**

To validate email addresses submitted to the Client to assist with the detection and prevention of fraud or financial crime, for the Client's internal business purposes only.

2.14 **MobileRisk:**

To validate telephone numbers submitted to the Client to assist with the detection and prevention of fraud or financial crime, for the Client's internal business purposes only.

2.15 **MobileSimSwap, MobileRedirect:**

For the detection and/or prevention of fraud and/or financial crime, for the Client's internal business purposes only.

2.16 **MobileKYC:**

For (i) identity verification and (ii) the detection and/or prevention of fraud and/or financial crime, in each case for the Client's internal business purposes only.

2.17 **Real Time Fraud Alerts:**

To aid in the identification and prevention of high fraud risks and identity theft for the Client's internal business purposes only.

BATCH SERVICES:

2.18 Together, the Output and the Report shall be used for the Client's own internal evaluation purposes only. For the avoidance of doubt, the Output and the Report shall not be used by the Client in a live production environment.

3. **SERVICE SCHEDULE DURATION**

3.1 **CallValidate International**

3.1.1 **Online Service**: Insert Details (Where Applicable)As set out in the Primary Schedule.

3.1.2 **Batch Service**: Insert Details (Where Applicable)As set out in the Primary ScheduleThis Service Schedule shall automatically terminate upon completion of the CallValidate International Service.

3.2 **CallValidate UK**

3.2.1 **Online Service**: Insert Details (Where Applicable)As set out in the Primary Schedule.

3.2.2 **Batch Service**: Insert Details (Where Applicable)As set out in the Primary ScheduleThis Service Schedule shall automatically terminate upon completion of the CallValidate UK Service.

3.3 As set out in the Primary Schedule.

4. **SERVICE CONDITIONS**

4.1 For the purpose of this Service Schedule, the following additional definitions shall apply:

4.1.1 Definitions applicable to the CallML element of CallValidate UK:

"**Full Register**" means the "register" as defined in the ER Regulations;

"**ML Regulations**" means, as relevant: (i) the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; (ii) any rules made by the Financial Conduct Authority under the Financial Services and Markets Act 2000 which relate to the prevention and detection of money laundering in connection with the carrying on of regulated activities by authorised persons; or (iii) any equivalent legislation in another jurisdiction.

4.1.2 Definitions applicable to the Bank element of CallValidate UK:

"**Extract**" means all information sourced from the ISCD Database that is contained in the Output;

"**ISCD**" means the Industry Sorting Code Directory;

"**ISCD Database**" means the VocaLink product by that name, consisting of a copy of a computer file of data relating to sort codes of financial institutions participating in UK Clearing Services or any other data taken from the computer file of ISCD and incorporated into any computer file produced or created by or on behalf of the Client;

"**Sorting Code**" means the code numbers issued from time to time by UK Payments for use in payment clearings operated by its members;

"**Sorting Code Data**" means the information that constitutes a sort code;

"**UK Clearing Services**" means each of the BACS Payment Services, the CHAPS Payment Services and the Cheque and Credit Clearing Services;

"**UK Payments**" means UK Payments Administration Limited whose registered office is at 2 Thomas More Square, London, E1W 1YN registered in England, number 1935025; and

"**VocaLink**" means VocaLink Limited of 1 Angel Lane, London EC4R 3AB, registered in England, company number 6119048.

4.1.3 Definitions applicable to the EmailRisk element of CallValidate UK:

"**EmailRisk Fraud Database**" means TransUnion's subcontractor's database of email addresses and associated information, which enables TransUnion to provide the EmailRisk Service to its clients;

"**EmailRisk Fraud Updates**" means evidence regarding email addresses determined to be associated with fraud or abuse;

"**EmailRisk Portal**" means the access point through which the Client may upload Fraud Updates directly to TransUnion's subcontractor

["**LexisNexis Risk Solutions UK Limited**" means LexisNexis Risk Solutions UK Limited, company number 07416642, with registered office address at Global Reach, Dunleavy Drive, Cardiff, CF11 0SN].

4.1.4 Definitions applicable to the MobileRisk element of CallValidate UK:

"**MobileRisk Fraud Database**" means TransUnion's subcontractor's database of telephone numbers and associated information, which enables TransUnion to provide the MobileRisk Service to its clients;

"**MobileRisk Fraud Updates**" means evidence regarding phone numbers determined to be associated with fraud or abuse;

"**MobileRisk Output Data**" means the output data provided to the Client as a result of using MobileRisk; and

"**MobileRisk Input Data**" means the individual telephone numbers that are made available by the Client to TransUnion for the purposes of performance of MobileRisk, whether input by the Client into the CallValidate UK input screen or delivered via the API. For the avoidance of doubt, no other information input into the CallValidate UK input screen shall constitute MobileRisk Input Data;

"**MobileRisk Portal**" means the access method through which the Client may upload Fraud Updates for onward transmission to TransUnion's subcontractor.

["**TeleSign**" means Telesign Corporation, a California company with its principal place of business at 13274 Fiji Way Suite 600, Marina del Rey CA 90292, USA].

4.1.5 Definitions applicable to the MobileSimSwap/MobileRedirect/MobileKYC element of CallValidate UK:

"**Bureau Privacy Notice**" means the TransUnion Bureau Privacy Notice, currently available at https://www.transunion.co.uk/legal/privacy-centre (or such replacement URL as notified to the Client from time to time);

"**CallValidate UK**" means TransUnion's online platform through which the Client shall access MobileSimSwap, MobileRedirect, MobileKYC;

"**Customer**" means, for the purposes of this Service Schedule, a customer of the Client whose personal data is contained in the Input and who may or may not be a Mobile Subscriber;

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

"**MNO**" means a Mobile Network Operator licensed to operate in the UK;

"**Mobile Network Operator**" means a telecommunications service provider organisation that provides wireless voice and data communication for its subscribed mobile users;

"**Mobile Subscriber**" means a consumer who contracts with one of the MNOs for the provision of mobile phone services;

"**OFCOM**" means the Office of Communications, being the UK government-approved regulatory and competition authority for the broadcasting, telecommunications and postal industries of the UK;

"**PAYGO Number**" means a mobile phone number associated with a 'pay as you go' phone;

"**Regulator**" means any government, quasigovernmental, statutory or regulatory body or any other competent authority or entity having responsibility for the regulation, governance or investigation of the business and activities of the Client, TransUnion, TransUnion's subcontractor or the MNOs, or the provision or use of the Services, including the FCA, Her Majesty's Revenue and Customs, the UK Information Commissioner and OFCOM; and

"**UK**" means the United Kingdom of Great Britain and Northern Ireland.

4.1.6 Definitions applicable to the DeviceRisk element of CallValidate UK:

"**Business Rules**" means the underlying business rules designed to assess the risk of fraud associated with a particular device and which are configurable to suit a particular sector and/or client risk profile;

"**DeviceRisk Output Data**" means the output data provided to the Client as a result of using the DeviceRisk Service;

"**DeviceRisk Input Data**" means the device technical data and user interaction attributes (including personal data) that is collected from individual

users of the Client's website and/or mobile application;
"**DeviceRisk Fraud Database**" means the database of known devices, which enables TransUnion to provide the DeviceRisk Service to its clients;
"**DeviceRisk Fraud Updates**" means evidence regarding accounts and devices determined to be associated with fraud or abuse;
"**Intelligence Center**" means the facility which allows the Client to obtain individual reporting, change Business Rules and contribute DeviceRisk Fraud Updates;
"**iovation**" means iovation Inc, a Delaware corporation with a place of business at 555 W. Adams St, Chicago, Illinois 60661, for the purposes of this Service Schedule, TransUnion's subcontractor.

4.1.7 Definitions applicable to the NCOA® element of CallValidate UK:
"**Applicant**" means an Applicant for, or prospective or existing customer of, the Client's products or services whose identity needs to be validated;
"**Applicant Record**" means the name and address (and, where available, the date of birth) of an Applicant which have been lawfully and fairly obtained by the Client for the purpose of verifying the Applicant's identity in relation to a product or service of the Client;
"**Data Protection Legislation**" means the Data Protection Act 2018, the General Data Protection Regulation (GDPR) (EU) 2016/679 and its UK equivalent, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 and any legislation and/or regulations implementing them or made in pursuance of them including where applicable the guidance and codes of practice issued by the Information Commissioner;
"**EEA**" means the European Economic Area which (as at the Agreement Signature Date) comprises the European Union Member States plus Iceland, Liechtenstein and Norway;
"**Intellectual Property Rights**" means all intellectual property rights including copyright and related rights, database rights, trade marks and trade names, patents, topography rights, design rights, trade secrets, know-how, and all rights of a similar nature or having similar effect which subsist anywhere in the world, whether or not any of them are registered and applications for registrations, extensions and renewals of any of them;
"**NCOA® Alert Database**" means a database containing Redirection Data;
"**New Address**" means the address specified by a redirection customer as that to which mail should be redirected;
"**Outputs**" means those data fields within or derived from the NCOA® Alert Database which TransUnion may incorporate into the creation of a Score or provide to the Client in accordance with paragraph 4.9.4;
"**Old Address**" means the address specified by a Redirection Customer as that from which mail should be redirected;
"**Permitted Purpose**" means the use of Scores and (where applicable) Outputs for the explicit purpose of preventing fraud or investigating whether fraud is being committed, relating to the Applicant or the Old Address in the course of validating information provided by the Applicant;
"**Redirection Data**" means data collected from the redirection forms completed by redirection customers who wish to use Royal Mail's service for the redirection of mail whereby mail which has been addressed to an Old Address is redirected to and delivered at the relevant New Address;
"**Reseller Agreement**" means Royal Mail's agreement with TransUnion under the terms of which Royal Mail licenses TransUnion to use NCOA® Alert Data to create, modify, provide and/or enhance the NCOA® Alert Service;
"**Royal Mail**" means Royal Mail Group Limited, a company registered in England & Wales under registered number 04138203 whose registered office is at 100 Victoria Embankment, London, EC4Y 0HQ; and
"**Score**" means the risk allocation assigned to an Applicant Record by TransUnion following a match against Redirection Data using a pre-determined scoring mechanism.

4.1.8 Definitions applicable to the Watchlist Screening element of CallValidate UK:
"**Dow Jones Factiva**" means Factiva Limited, incorporated in England and Wales (registered company number 3773253) whose registered and principal place of business is at The News Building, 1 London Bridge Street, London SE1 9GF;
"**Error Message**" means an error message that *"Watchlist_0X: Cannot complete CallValidateWatchlistScreening check"* or a message giving equivalent information;
"**ML Regulations**" means, as relevant: (i) the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; (ii) any rules made by the Financial Conduct Authority under the Financial Services and Markets Act 2000 which relate to the prevention and detection of money laundering in connection with the carrying on of regulated activities by authorised persons; or (iii) any equivalent legislation in another jurisdiction;
"**Sanctions Legislation**" means the Sanctions and Anti-Money Laundering Act 2018 and Economic Crime (Transparency and Enforcement) Act 2022 and any regulations made under those Acts;
"**Third Party Data**" means the data received from the Third Party Subcontractor through the provision of the Third Party Service;
"**Third Party Service**" means the service provided to TransUnion by the Third Party Subcontractor; and
"**Third Party Subcontractor**" means Dow Jones Factiva or such other reputable third party subcontractor as may be appointed by TransUnion in the future to provide the Third Party Service.
"**Watchlist Screening**" means the part of the Output which uses Third Party Data to identify an individual as a possible Politically Exposed Person ("**PEP**"), family member or known close associate of a PEP (each as defined in the ML Regulations) or subject to financial sanctions, and which returns details of these potential matches and/or where such individuals are present on other special interest, official or exclusion lists.

4.2 **These Service Conditions shall apply in respect of the Services.**

4.2.1 In respect of the CallValidate UK Service, the Client grants to TransUnion a non-exclusive, irrevocable, perpetual licence to copy, store, use and sub-license the Input (including the electronic mail and internet protocol addresses that form part of the Input) to enable TransUnion to provide services to its clients in which the Input is used to assist with identity verification and prevention of fraud/money laundering, tracing debtors, tracing existing customers for the purpose of customer management or asset reunification, and prevention and detection of crime.

4.2.2 Additionally, where the:

- EmailRisk module is taken, the licence granted to TransUnion at 4.2.1 shall include an irrevocable, perpetual licence for its subcontractor to retain and use the Input (and, where the Client contributes EmailRisk Fraud Updates via the EmailRisk Portal, the EmailRisk Fraud Updates also) to assist the subcontractor in improving the EmailRisk Fraud Database;
- MobileRisk module is taken, the licence granted to TransUnion at 4.2.1 shall include an irrevocable, perpetual licence for its subcontractor to retain and use the MobileRisk Input Data (and, where the Client contributes MobileRisk Fraud Updates via the MobileRisk Portal, the MobileRisk Fraud Updates also) to assist the subcontractor in improving the MobileRisk Fraud Database;
- DeviceRisk module is taken, the licence granted to TransUnion at 4.2.1 shall include a non-exclusive, irrevocable, perpetual licence for iovation to retain and use the DeviceRisk Input Data and the DeviceRisk Fraud Updates to assist with identity verification and prevention of fraud/money laundering.

4.2.3 For the avoidance of doubt, the Input (or any part thereof) will not be used by TransUnion or any subcontractor(s) (as the case may be), to initiate contact with the Client's customers for direct marketing purposes.

4.2.4 Paragraphs 4.2.1 and 4.2.3 shall survive the expiry or termination of this Agreement.

4.2.5 Paragraphs 4.2.1[LAWYER TO DELETE AS APPROPRIATE]:, 4.2.2 and 4.2.3 shall survive the expiry or termination of this Agreement.

4.2.6 The Client acknowledges that:

TransUnion

(a) in respect of the CallValidate International Service;
(b) in respect of the MobileRisk Service;
(c) in respect of the DeviceRisk Service;
(d) in respect of the MobileSimSwap, MobileRedirect, MobileKYC Service;
(e) in respect of the Watchlist Screening element of the CallValidate UK Service;

TransUnion, and to the extent applicable, its subcontractor(s), may be required to transfer parts of the Input or DeviceRisk Input Data (including personal data contained within such Input) to third parties located in countries or territories outside of the EEA of both the UK and/or EEA. The licence granted by the Client in clause 6.3 of the General Terms, is granted in full contemplation of and agreement to, such transfers. Any such transfers shall be performed in accordance with the Data Protection Legislation.

4.2.7 The Client warrants to TransUnion that, in compliance with the Applicable Law (including the Data Protection Legislation), applicable consent has been obtained, and appropriate notices have been given to its customers, that the data provided by those customers, including the DeviceRisk Fraud Updates, may be processed in the manner described in **[LAWYER TO DELETE AS APPROPRIATE]**: paragraph 4.2.1/paragraphs 4.2.1, 4.2.2, 4.2.6 and 4.12.4/paragraphs 4.2.1 and 4.2.2 above and 4.15.1 below. Such notice shall include (i) a link to the TransUnion Bureau Privacy Notice, currently available at https://www.transunion.co.uk/legal-information/bureau-privacy-notice (or such replacement URL as notified to the Client from time to time); and/or (ii) in respect of the DeviceRisk element of the CallValidate UK Service, a link to the iovation privacy policy currently available at https://www.transunion.com/privacy/iovation (or such replacement URL as notified to the Client from time to time).

4.2.8 The Client warrants to TransUnion that, in compliance with the Applicable Law (including the Data Protection Legislation), applicable consent has been obtained, and appropriate notices have been given to its customers, that the data provided by those customers, may be processed in the manner described in paragraph 4.2.1. Such notice shall include a link to the TransUnion Bureau Privacy Notice, currently available at https://www.transunion.co.uk/legal-information/bureau-privacy-notice (or such replacement URL as notified to the Client from time to time).

4.2.9 Details of the configuration of the Services for the Client shall be agreed between the parties.

4.2.10 The Client agrees that, subject to paragraph 4.2.11 below, it shall only use the CallValidate UK Service (including the elements set out in paragraph 1.2 1.12 1.2 and 1.12 above) in respect of customers who are residents of the UK, Isle of Man or the Channel Islands.

4.2.11 The Client is also permitted to use the [EmailRisk], [MobileRisk] and/or [DeviceRisk] elements of the CallValidate UK Service in respect of customers who are residents of the EEA or the USA.

4.2.12 The Client acknowledges that the CallValidate UK Service is not intended to be indicative of a customer's creditworthiness or eligibility for insurance. Without prejudice to paragraph 2 of this Service Schedule (Permitted Purpose) and clause 5.1.1 of the General Terms, the Client warrants that it shall not use the Output from the CallValidate UK Service as a factor in establishing any customer's eligibility for credit or insurance.

4.2.13 The Client shall not use the CallValidate UK Service as the sole basis for any business decision. Without prejudice to clause 8.10 of the General Terms, the Client shall not use the CallValidate UK Service (including any Output) to make a decision based solely on automated processing (including profiling) in relation to a data subject where such decision produces legal effects concerning that data subject or similarly significantly affects that data subject (including entirely preventing a data subject from signing up or accessing the Client's services) except where the Client is permitted to do so pursuant to the Data Protection Legislation. Where it is so permitted to make such decision, the Client shall at all times comply with all relevant requirements as set out under the Data Protection Legislation in relation to that data subject's rights and freedoms and legitimate interests in connection with that decision.

4.2.14 Prohibited Use (as defined in the General Terms) for the purposes of this Service Schedule shall additionally include the following:

4.2.14.1 any activity or material which promotes or encourages illicit or controlled drugs or substances (excluding medicines or pharmaceuticals); and/or

4.2.14.2 sale of weapons, firearms, explosives, replica weapons or replica firearms (excluding sale of knives and/or tools used for DIY, gardening, kitchen or trade purposes, sold through established e-commerce channels).

4.2.15 If the Client uses the Services or the Output in connection with any Prohibited Use described in paragraph 4.2.11 or any Prohibited Material, without prejudice to its other remedies TransUnion may terminate the Services and/or (regardless of this Service Schedule having already expired or terminated) any continuing licence in respect of CallValidate under clause 5.1.2 immediately on notice to the Client.

4.3 **These Service Conditions shall apply in respect of the Age Verification Standard element of the CallValidate UK Service.**

4.3.1 The Client shall ensure that the Input for each Age Verification Standard enquiry contains the date of birth as presented by the relevant customer.

4.4 **These Service Conditions shall apply in respect of the CallML element of the CallValidate UK Service.**

4.4.1 The CallML check contains the Full Register and must therefore only be used by the Client in accordance with the ER Regulations and only where it is meeting any obligations contained in the ML Regulations.

4.5 **These Service Conditions shall apply in respect of the Bank element of the CallValidate UK Service.**

4.5.1 As between the Client and TransUnion, the Extract shall be the property of VocaLink and except as provided by the terms of this Agreement (and s.296A of the Copyright Designs and Patents Act 1988) the Client shall have no rights to copy, modify, develop or adapt the Extract or to sell, dispose of or transfer the Extract or any copies thereof in the possession of the Client.

4.5.2 All Extracts and related data licensed to the Client are provided in an "as is" state. No warranty or indemnity of any kind whatsoever is given by TransUnion or its suppliers in respect of the Extract and all conditions and warranties express or implied or otherwise are hereby expressly excluded to the fullest extent permitted by law.

4.5.3 The Client warrants that the Input is accurate at the date of supply to TransUnion and will not include any information or material, any part of which, or the accessing of which or use of which would be a criminal offence or otherwise unlawful. In particular, the Client warrants that all necessary licences and consents (if any, and including but not limited to those from owners of copyrights) have been obtained.

4.5.4 The Client acknowledges that all intellectual property rights including but not limited to copyright and other intellectual property rights in the ISCD Database are owned by VocaLink and that all intellectual property rights in the Sorting Code, Sorting Code Data, and the Industry Sorting Code Directory are owned by UK Payments.

4.5.5 No title or rights of ownership, copyright or any other intellectual property rights in the ISCD Database, Sorting Code, Sorting Code Data, and the Industry Sorting Code Directory are or will be transferred to the Client.

4.5.6 The Client will ensure that all of its relevant employees are advised that the ISCD Database and all intellectual property rights in it are the property of VocaLink and the Client will use all reasonable endeavours to ensure that its employees comply with all of the terms and conditions of this Agreement.

4.5.7 The Client shall ensure that any permitted copies of the Extract will incorporate an appropriate notice indicating that copyright in the ISCD Database is vested in VocaLink.

4.5.8 The Client acknowledges that its right to use the Extract (and any copies) may be terminated on written notice at any time in the event that TransUnion or its licensors cease, for any reason, to have the right to make the Extract available or if the Client fails to abide by these Service Conditions for CallValidate UK.

4.5.9 To the maximum extent permitted by law, the Client acknowledges that the data suppliers to TransUnion (including VocaLink) and their respective officers, employees, agents and licensors have no liability to it whatsoever in connection with this Agreement or the Client's use of the ISCD

Database, card verification data or any other part of the Output.

4.6 **This Service Condition shall apply in respect of the Card Live element of the CallValidate UK Service.**

4.6.1 Where the CallValidate UK Service includes the Card Live element (as indicated in the Payment Schedule) then the Client shall ensure that each cardholder in respect of whom the Client requests Card Live verification (i) consents to such verification being carried out; and (ii) agrees to the information concerning, and the results of, the verification being passed to the Client and any third parties processing such data on behalf of the Client.

4.7 **These Service Conditions shall apply in respect of the Bank Account Premium element of the CallValidate UK Service.**

4.7.1 The Client acknowledges that to deal with the sensitivities that some data subjects may have regarding the use of their data for ID verification purposes, the Client shall offer alternative methods by which a data subject can verify their identity and shall not discriminate against a data subject because of their refusal to use or permit the use of electronic ID verification systems.

4.7.2 Where the CallValidate UK Service includes the Bank Account Premium element (as indicated in the Payment Schedule) then the Client agrees to receive the Output in respect of Bank Account Premium via the CallValidate UK scorecard only until such time as the Client upgrades to the latest version of the API. The timetable for such upgrade shall be agreed between the parties.

4.8 **These Service Conditions shall apply in respect of the CallValidate3D element of the CallValidate UK Service.**

4.8.1 The Client acknowledges that the CallValidate3D element of the CallValidate UK Service may use Closed User Group data (as defined in, and subject to the terms of the paragraph entitled "**Closed User Group Data**" in the Primary Schedule).

4.9 **These Service Conditions shall apply in respect of the NCOA® Alert element of the CallValidate UK Service.**

4.9.1 The use by the Client of the NCOA® Alert Service is also subject to the following terms ("**Minimum Terms**") which are imposed by Royal Mail. In the event of any inconsistency between the definitions set out in these Service Conditions and those in the General Terms, the definitions in these Minimum Terms shall apply to the extent of any inconsistency. The Client acknowledges and agrees that in respect of the NCOA® Alert Service, the Permitted Purpose set out in these Service Conditions overrides the Permitted Purpose contained in this Service Schedule.

4.9.2 Licence

4.9.2.1 In consideration of the Client complying with these Minimum Terms, TransUnion grants to the Client a non-exclusive, non-transferable, revocable sub-licence in the United Kingdom and the EEA to access and use the Scores and Outputs for the Permitted Purpose (as defined in these Service Conditions) only.

4.9.2.2 At any time during the term of this Agreement, on the provision of reasonable written notice from TransUnion, the Client shall respond to Royal Mail's reasonable questions for the purpose of verifying the Client's compliance with these Minimum Terms.

4.9.3 Scores

4.9.3.1 Scores are compiled by TransUnion using the results of matching Redirection Data and third party data against each Applicant record, and are therefore not based solely on Redirection Data. Royal Mail gives no assurance, commitment or warranty as to the accuracy or validity of any Score.

4.9.4 Outputs

4.9.4.1 Outputs relating to a particular Applicant Record indicating that a match has been achieved against the Redirection Data will only be made available to the Client where TransUnion achieves a name and address level match when processing the Applicant Record against Redirection Data.

4.9.4.2 The Client may only use Outputs for a one-off Applicant validation and only in accordance with the Permitted Purpose. All Outputs from the NCOA® Alert Service must be deleted from the Client's systems within seven days of receipt.

4.9.4.3 The Client must not modify or alter any Outputs or manipulate such Outputs other than to develop a risk based score in relation to the relevant Applicant. This score must include third party data analysis as well as Output analysis before a decision is made in relation to the relevant Applicant. Royal Mail gives no assurance, commitment or warranty as to the accuracy or validity of any such score.

4.9.5 Liability of Royal Mail

4.9.5.1 The Client agrees that Royal Mail will not be liable for any loss or damage (whether direct or indirect) however arising from the use by the Client of any Scores or Outputs, with the exception of death or personal injury caused by Royal Mail's negligence.

4.9.5.2 The Client acknowledges that Royal Mail will not be liable to the Client in respect of its use of the NCOA® Alert Service.

4.9.5.3 The Client acknowledges that Royal Mail will not be obliged in any circumstances to provide Redirection Data or related services directly to the Client.

4.9.6 Property Rights in Redirection Data

4.9.6.1 The Client acknowledges and agrees that the NCOA® Alert Service contains NCOA® Alert Data, which is licensed to TransUnion by Royal Mail Group Limited.

4.9.6.2 The Intellectual Property Rights in any Outputs supplied to the Client as part of its use of the NCOA® Alert Service shall remain at all times the property of Royal Mail.

4.9.6.3 The Client will not do or permit the doing of anything within its control which will prejudice in any way whatsoever the name of Royal Mail or the rights of Royal Mail in the Outputs and will give immediate notice to Royal Mail upon the Client becoming aware of anything which may prejudice the name of Royal Mail or the rights of Royal Mail in the Outputs.

4.9.6.4 The Client undertakes to Royal Mail that it will give immediate notice to Royal Mail upon its becoming aware of any unauthorised use of any Scores, Outputs or any other Intellectual Property Rights of Royal Mail.

4.9.6.5 Royal Mail may bring any action for any such unauthorised use on behalf of itself and at its cost and the Client shall co-operate fully in any such action. The Client is not granted any separate right of action relating to Royal Mail's Intellectual Property Rights in respect of any such unauthorised use and disclaims any such separate right that it may have insofar as such a disclaimer is permitted by law.

4.9.7 Data Protection

4.9.7.1 The Client acknowledges that these Minimum Terms are structured in order to comply with the Data Protection Legislation.

4.9.7.2 The Client undertakes that it will not do or omit to do any act which would place it or Royal Mail in breach of the Data Protection Legislation.

4.9.7.3 The Client acknowledges and agrees that it is the factual arrangement between parties which dictates the role and status of each party under Data Protection Legislation in respect of processing any personal data. Notwithstanding the foregoing, Royal Mail anticipates that Royal Mail and the Client shall, each separately determine the purposes for which and the manner in which any personal data is required to be processed, and therefore, are each a data controller in respect of such personal data.

4.9.7.4 Each party undertakes to the other that it will duly observe all its obligations under the Data Protection Legislation which arise in connection with these Minimum Terms.

4.9.7.5 The Client must not disclose or pass any Outputs outside the United Kingdom and EEA without the prior written consent of Royal Mail.

4.9.8 Information security

4.9.8.1 The Client in relation to the security of Outputs and Scores whilst in the Client's possession shall:

4.9.8.1.1 agree to comply with TransUnion's information security policy and any other information security requirements, policies or procedures notified by TransUnion to the Client;
4.9.8.1.2 protect all Outputs and Scores from unauthorised access, damage, disclosure, loss and interference, whether intentional or accidental;
4.9.8.1.3 ensure that all allowed destruction of all Outputs and Scores is carried out in a manner that avoids unauthorised or accidental disclosure of the Outputs and Scores;
4.9.8.1.4 ensure that all Outputs and Scores stored in paper form or in electronic storage devices, once no longer needed, are shredded or disposed of in a secure manner; and
4.9.8.1.5 notify Royal Mail of any unauthorised or unlawful disclosure or use of the Outputs and Scores of which the Client becomes aware.
4.9.9 General
4.9.9.1 TransUnion may terminate this Agreement or the NCOA® Alert Service (including the provision of Outputs and Scores) with immediate effect if the Client brings Royal Mail into disrepute or fails to comply with these Minimum Terms.
4.9.9.2 If the Reseller Agreement expires or is terminated for any reason, the provision of the NCOA® Alert Service will automatically be terminated.
4.9.9.3 The Client acknowledges and agrees that these Minimum Terms are given for the benefit of Royal Mail and that Royal Mail may enforce the benefits conferred on it under these Minimum Terms as if it were a party to this Agreement so far as it relates to the NCOA® Alert Service in accordance with the Contracts (Rights of Third Parties) Act 1999. The Client further acknowledges and agrees that Royal Mail shall bring any action for any unauthorised use of its Intellectual Property Rights on its own behalf. This paragraph 4.9.9.3 shall be an express exception to clause 23.1 of the General Terms in respect of the Contracts (Rights of Third Parties) Act 1999.
4.9.9.4 Except as set out at paragraph 4.9.9.3 above, a person who is not a party to this Agreement may not enforce any of its provisions under the Contracts (Rights of Third Parties) Act 1999.
4.9.9.5 Except to the extent otherwise permitted by the Reseller Agreement these Minimum Terms may not be varied by the Client or TransUnion without the prior written consent of Royal Mail. This paragraph 4.9.9.5 shall be an express exception to clause 23.2 of the General Terms.
4.9.9.6 These Minimum Terms are governed by English law.
4.9.10 The Client acknowledges that the NCOA® Alert Service shall not include the use of or the provision of the Redirection Data in any circumstances in which it is envisaged under Chapter II of the Regulation of Investigatory Powers Act 2000 ("**RIPA**") that a notice would be issued by or on behalf of the Client under and in accordance with section 22 of that Act requiring the disclosure of the relevant Redirection Data (taking into account the Code of Practice on Acquisition and Disclosure of Communications Data issued pursuant to section 71 of that Act).
4.9.11 The Client agrees that it does not require the provision of any Redirection Data such that it is envisaged under Chapter II of the Regulation of Investigatory Powers Act 2000 that a notice will be issued under section 22 of that Act requiring the disclosure of the relevant Redirection Data for any purpose and the Client undertakes that if it shall require any Redirection Data as so envisaged under RIPA, it will use and apply the notice procedure provided for in section 22 of that Act to obtain such Redirection Data.
4.9.12 The parties agree that any pre-existing service level targets in force between the Client and TransUnion in respect of the CallValidate UK Service do not apply to the provision of the NCOA® Alert element.

4.10 **These Service Conditions shall apply in respect of the CallID (Employment Check) via CallValidate UK Service.**
4.10.1 The Client shall make each data subject aware that the search footprint retained by TransUnion in respect of a search made using the CallValidate UK Service will show that an identity check has been performed.

4.11 **These Service Conditions shall apply in respect of the Watchlist Screening element of the CallValidate UK Service.**
4.11.1 The Client acknowledges that Watchlist Screening relies upon the provision of the Third Party Service. To the extent that the Third Party Data is not available, TransUnion will return an Error Message to the Client. For the avoidance of doubt, if an Error Message is returned, the Client will not be charged for Watchlist Screening.
4.11.2 TransUnion grants to the Client a non-exclusive, non-transferable, non-sub licensable, non-assignable licence to use the Third Party Data subject to the terms and conditions of this Service Schedule. For the avoidance of doubt, the Client shall not acquire any ownership rights in the Third Party Data.
4.11.3 The Client shall use the Output strictly in accordance with the Permitted Purpose and all Applicable Law and regulations and shall ensure that it is accessed only by Client Users.
4.11.4 The Client shall assume full responsibility and liability for the acts and omissions of all Client Users as if such acts and omissions were committed or made by the Client as well as ensuring that all Client Users use the passwords only on a dedicated basis for the Client or Authorised Group Company as applicable.
4.11.5 The Client acknowledges that the TransUnion's subcontractor is not a "credit reference agency" as defined in section 145(8) of the Consumer Credit Act 1974 and that the Third Party Data does not constitute a "consumer report" or "investigative consumer report", as such terms are defined in the US Fair Credit Reporting Act, 15 U.S.C. §1681, et seq. For the avoidance of doubt, the Client shall not use the Output in isolation for determining or taking adverse action in relation to an individual's eligibility for credit, insurance or employment save where there is a confirmed positive match that the individual is subject to financial sanctions as defined in the ML Regulations.
4.11.6 Except to the extent allowable under the Permitted Purpose, the Client and/or Client Users shall not: (i) reproduce, distribute, display, sell, publish, broadcast or circulate the Output to any third party that is not an Authorised Group Company, nor make the Output available for any such use; or (ii) create or store in electronic form any library or archive of the Output save that, and notwithstanding anything to the contrary, the Client shall be entitled to retain copies of the Output necessary for archival, regulatory and/or compliance purposes. The Client's right to retain such copies as set out above shall survive termination/expiration of this Service Schedule provided that it no longer actively uses the Output.
4.11.7 Each party shall comply with its obligations under the Data Protection Legislation in relation to any personal data processed in connection with this Agreement. Without prejudice to the foregoing, the Client acknowledges that the Output under this Service Schedule may involve the processing of special categories of personal data and/or personal data relating to criminal convictions and offences pursuant to Articles 9 and 10 of the GDPR.
4.11.8 The Client shall promptly notify TransUnion if it: (i) cannot for any reason comply with its obligations under paragraph 4.11.7 above; or (ii) becomes aware of any circumstance or change in the Data Protection Legislation that is likely to have a substantial adverse effect on its ability to meet its obligations under paragraph 4.11.7.
4.11.9 Without prejudice to clause 5.6 of the General Terms, TransUnion does not warrant that Watchlist Screening is derived from a complete or accurate archive of every individual defined as a PEP, family member or known close associate of a PEP under the ML Regulations. TransUnion does not imply any negative inferences about individuals referred to within the Output merely due to the fact they have been flagged as a possible PEP, family member or known close associate of a PEP.
4.11.10 The parties agree that any pre-existing service level targets in force between the Client and TransUnion in respect of the CallValidate UK Service do not apply to the provision of the Watchlist Screening element.

4.12 **These Service Conditions shall apply in respect of the DeviceRisk element of the CallValidate UK Service.**
4.12.1 The DeviceRisk Service and the DeviceRisk Output Data are licensed to the Client by TransUnion on a non-exclusive basis only.
4.12.2 The Client agrees to install the Device Identifying Software on its website and/or mobile application and utilise such Device Identifying Software on

a non-exclusive basis.

4.12.3 The Client agrees that TransUnion and/or iovation will retain all ownership rights (including but not limited to any copyright, patent, trade secret, trade mark or other proprietary and/or intellectual property rights) in and to the Device Identifying Software, the DeviceRisk Service, the DeviceRisk Output Data and the DeviceRisk Fraud Database (including but not limited to any components thereof, any information contributed to the DeviceRisk Fraud Database as a result of the performance of this Agreement and any adaptation of the Device Identifying Software or the DeviceRisk Service to meet the Client's specifications, unless the adaptation incorporates intellectual property of the Client in which case such intellectual property will remain the Client's property) (together the "**DeviceRisk Elements**"). To the extent that any such rights may have vested in it, the Client hereby assigns to TransUnion all existing and future intellectual property rights in the DeviceRisk Elements and all materials embodying such rights to the fullest extent permitted by law.

4.12.4 The Client acknowledges that the DeviceRisk Service may use first party cookies (set by the Client) and third party cookies (set by TransUnion/iovation) for its data capture process.

4.12.5 The Client shall provide (or will procure that a third party acting on its behalf will provide) DeviceRisk Fraud Updates on a regular basis by submitting such evidence via the Intelligence Center.

4.12.6 The Client acknowledges that neither TransUnion nor its subcontractor make any warranties or representations (i) as to the suitability of the DeviceRisk Service and DeviceRisk Output Data for any particular purpose; (ii) as to the accuracy or completeness of the DeviceRisk Output Data; or (iii) that the DeviceRisk Service will be uninterrupted or continuously available. For the avoidance of doubt, unless expressly stated to the contrary, all warranties provided by TransUnion as part of the General Terms are provided by TransUnion only.

4.12.7 The Client shall not create or attempt to create (or permit others to create or attempt to create), by reverse engineering or otherwise, the source programs or any part thereof from the object programs or from any other information made available to it by TransUnion or its subcontractor under this Agreement and shall not decompile, disassemble, modify, alter or create derivative works of the Service. Liability for a breach of this Service Condition shall be unlimited, notwithstanding the liability provisions set out in clause 10 of the General Terms.

4.12.8 Nothing contained in this Agreement shall be construed as granting or conferring any right, title, or interest, in any proprietary information, patent, trade mark, copyright, trade secret or other proprietary right in the DeviceRisk Service or Device Identifying Software that is now or subsequently owned by iovation or TransUnion.

4.12.9 Without prejudice to clause 5.7 of the General Terms, if the DeviceRisk Output Data contains a system error message, this is an indicator that either the system has timed out or that there is an internal system issue and no assumption should be made by the Client (on the basis of this error message) as to the fraud risk associated with the particular DeviceRisk Input Data that resulted in the system error message.

4.12.10 The Client acknowledges that TransUnion is the first line of support and that it will request assistance from TransUnion in respect of any issues that arise in relation to the Services, including for the avoidance of doubt the Device Identifying Software. The Client further agrees that it will not contact TransUnion's subcontractor directly except with the prior agreement of TransUnion.

4.12.11 The parties agree that any pre-existing service level targets in force between the Client and TransUnion in respect of the CallValidate UK Service do not apply to the provision of the DeviceRisk element.

4.13 **These Service Conditions shall apply in respect of the EmailRisk element of the CallValidate UK Service.**

4.13.1 The Client may contribute to the EmailRisk Fraud Database by submitting (or procuring that a third party acting on its behalf shall submit) EmailRisk Fraud Updates via the Portal.

4.13.2 For the avoidance of doubt, and without prejudice to clause 5.7 of the General Terms, if the Output contains a system error message, this is either an indicator that the system has timed out or that there is an internal system issue and no assumption should be made by the Client (on the basis of this error message) as to the fraud risk associated with the particular email address that resulted in the system error message.

4.13.3 The parties agree that any pre-existing service level targets in force between the Client and TransUnion in respect of the CallValidate UK Service do not apply to the provision of the EmailRisk element.

4.14 **These Service Conditions shall apply in respect of the MobileRisk element of the CallValidate UK Service.**

4.14.1 The Client may contribute to the MobileRisk Fraud Database by submitting (or procuring that a third party acting on its behalf shall submit) MobileRisk Fraud Updates via the Portal.

4.14.2 The Client agrees that TransUnion and/or its subcontractor will retain all ownership rights (including but not limited to any copyright, patent, trade secret, trade mark or other proprietary and/or intellectual property rights) in and to MobileRisk and the MobileRisk Output Data.

4.14.3 For the avoidance of doubt, and without prejudice to clause 5.7 of the General Terms, if the MobileRisk Output Data contains a system error message, this is either an indicator that the system has timed out or that there is an internal system issue and no assumption should be made by the Client (on the basis of this error message) as to the fraud risk associated with the particular telephone number that resulted in the system error message.

4.14.4 The parties agree that any pre-existing service level targets in force between the Client and TransUnion in respect of the CallValidate UK Service do not apply to the provision of the MobileRisk element.

4.15 **These Service Conditions shall apply in respect of the MobileSimSwap, MobileDirect and MobileKYC element(s) of the CallValidate UK Service.**

4.15.1 The Client acknowledges that, in order to provide the MobileSimSwap, MobileDirect and MobileKYC elements to the Client, TransUnion will transfer the Input to a subcontractor appointed by TransUnion which will (i) ascertain which is the relevant MNO and (ii) check the Input against data held by such MNO. The licence granted by the Client at clause 6.3 of the General Terms is granted in full contemplation of and agreement to such transfers.

4.15.2 Without prejudice to clause 6 and notwithstanding clause 9 of the General Terms, TransUnion may be required to provide reasonable feedback to its subcontractor upon reasonable request including, without limitation, usability reports, error notifications and test results and the subcontractor will own all Intellectual Property Rights, title and interest in and to any and all feedback, reports, analyses, recommendations and all other materials created as part of the feedback, whether created or gathered by TransUnion during the course of or as a result of this Agreement.

4.15.3 The Client agrees that TransUnion and its subcontractor may collect, store, host, access, use, reproduce and modify, during and after the term of this Agreement, any and all data, inputs, responses and other information concerning the Client's use of the MobileSimSwap, MobileDirect and MobileKYC elements for the purposes of conducting data and usage analytics, parsing routes, data modelling and other analyses in order to (i) prepare reports for internal use, and (ii) test, evaluate, develop and enhance their services, and the subcontractor may share such data with the MNOs for the purposes of developing and distributing products and services that incorporate or use such data solely for the purposes of fraud, risk and authentication. Such data or information shall not include any personal data processed as part of the provision of the MobileSimSwap, MobileDirect and MobileKYC elements.

4.15.4 To the extent expressly required under Data Protection Legislation, the Client shall obtain and retain adequate records of any consents received from Customers relating to the processing of the Customers' personal data and shall retain such consents in accordance with Data Protection Legislation.

4.15.5 The Client shall not:

4.15.5.1 transfer the Output to, nor permit access to the Output from, any country outside of the UK and/or the EEA without TransUnion's prior written consent;

4.15.5.2 permit the Output to be used for purposes of product evaluation, benchmarking or other comparative analysis intended for publication without the prior written consent of TransUnion; or

4.15.5.3 use the MobileSimSwap, MobileDirect and MobileKYC elements or Output to create a consumer report or for use by a consumer reporting agency for the purpose of creating a consumer report as defined under 15 USC §1681a or for any other purpose to the extent it would cause TransUnion or its subcontractor to be subject to the Fair Credit Reporting Act ("**FCRA**") or any similar laws or regulations, or for FCRA permissible purposes.

4.15.6 The Client shall ensure that its personnel (and the personnel of any authorised processor employed by the Client) are bound by industry standard confidentiality obligations.

4.15.7 At the request of TransUnion, the Client shall provide written evidence of the measures implemented to comply with the requirements set out in paragraphs 4.2.7, 4.15.4 and 4.15.6 above for onward transfer to the MNOs.

4.15.8 The Client agrees to cooperate fully with TransUnion in relation to any complaint made by a data subject and/or any enquiry by a Regulator in relation to the MobileSimSwap, MobileDirect and MobileKYC elements.

4.15.9 The Client shall promptly notify TransUnion upon becoming aware of a data breach that impacts any personal data contained in the Output which is not included in the Input.

4.15.10 The Client acknowledges that a "*numbernotfound*" does not necessarily indicate an invalid mobile phone number and is not on its own an indicator of fraud.

4.15.11 Without prejudice to TransUnion's right to suspend access to the MobileSimSwap, MobileDirect and MobileKYC elements pursuant to the General Terms, the Client acknowledges and agrees that one or all of the MNOs may suspend the provision of their services to TransUnion or its subcontractor. In such circumstances, all or part of the MobileSimSwap, MobileDirect and MobileKYC elements may be impacted and could result in the MobileSimSwap, MobileDirect and MobileKYC elements being partially or wholly suspended.

4.15.12 The parties agree that any pre-existing service level targets in force between the Client and TransUnion in respect of the CallValidate UK Service do not apply to the provision of the MobileSimSwap, MobileDirect and MobileKYC elements.

4.16 **This Service Condition shall apply in respect of the Activity History element(s) of the CallValidate UK Service.**

4.16.1 Without prejudice to clause 5.7 of the General Terms, if the Output contains an unknown result or 'U', this is an indicator that TransUnion cannot verify that activity has or has not taken place on the relevant account in the relevant period. No assumption should be made by the Client as to the fraud risk associated with the relevant account or customer based on such Output.

SERVICE SCHEDULE
CLEARKEY (ONLINE)

Commented [MS2]: This Service Schedule contains all options - the Schedule will need to be tailored to reflect the particular options and permitted purposes applicable for the relevant client at Call-Off stage. Therefore, not all provisions in this Service Schedule will be applicable at the Call-Off stage.

1. **DESCRIPTION OF THE SERVICES**

In this Service Schedule, the Services shall comprise the following:

1.1 The provision of software (including, where appropriate, a software development kit) designed to collect certain device technical data and user interaction attributes (the "**Device Identifying Software**"), which must be installed on the Client's website and/or mobile app;
1.2 Integration support;
1.3 ClearKey, delivered via iovation's API (the "**ClearKey Service**");
1.4 Access to the Intelligence Center;
1.5 Set up and maintenance of an API in respect of the ClearKey Service;
1.6 API access to a data storage facility that allows the Client to download certain information on transactions they have processed through the ClearKey Service ("**Transaction Storage Service**").

2. **PERMITTED PURPOSE**

To assist the Client in identifying the likelihood that the device being used to access an account via the Client's website/mobile app matches a device that has been registered to that account, for the Client's internal business purposes only.

3. **SERVICE SCHEDULE DURATION**

3.1 Insert Details (Where Applicable)As set out in the Primary Schedule.

4. **SERVICE CONDITIONS**

These Service Conditions shall apply in respect of the Services.

4.1 In respect of these Service Conditions, the following definitions apply:

"**Business Rules**" means the underlying business rules designed to assess the likelihood that the device being used to access an account matches a device that has been registered to that account;

"**ClearKey Output Data**" means the output data provided to the Client as a result of using the ClearKey Service;

"**ClearKey Input Data**" means the device technical data and user interaction attributes (including personal data) that is collected from individual users of the Client's website and/or mobile app;

"**Fraud Database**" means the database of known devices, which enables TransUnion to provide the ClearKey Service to its Clients;

"**Fraud Updates**" means evidence regarding accounts and devices determined to be associated with fraud or abuse;

"**Intelligence Center**" means the facility which allows the Client to obtain individual reporting, view Transaction Insight Data, change Business Rules and contribute Fraud Updates;

"**iovation**" means iovation Inc, a Delaware corporation with a place of business at 555 W. Adams St, Chicago, Illinois 60661, for the purposes of this Service Schedule, TransUnion's subcontractor; and

"**Transaction Insight Data**" means the optional application and/or transaction data (including personal data such as email address and/or billing address) that are collected from or associated with individual users of the Client's website and/or mobile app.

4.2 The ClearKey Service and the ClearKey Output Data are licensed to the Client by TransUnion on a non-exclusive basis only.

4.3 The Client agrees to install the Device Identifying Software on its website and/or mobile app and utilise such Device Identifying Software on a non-exclusive basis.

4.4 The Client acknowledges that the provision of the ClearKey Service requires TransUnion and/or its subcontractor to transfer the ClearKey Input Data and the Transaction Insight Data (including personal data contained within such Input) to third parties located in countries or territories outside of both the United Kingdom and European Economic Area. The licence granted by the Client at clause 6.3 of the General Terms is granted in full contemplation of and agreement to such transfers. Any such transfers shall be performed in accordance with the Data Protection Legislation.

4.5 The Client agrees that TransUnion and/or iovation will retain all ownership rights (including but not limited to any copyright, patent, trade secret, trade mark or other proprietary and/or intellectual property rights) in and to the Device Identifying Software, the ClearKey Service, the ClearKey Output Data and the Fraud Database (including but not limited to any components thereof, any information contributed to the Fraud Database as a result of the performance of this Agreement and any adaptation of the Device Identifying Software or the ClearKey Service to meet the Client's specifications, unless the adaptation incorporates intellectual property of the Client in which case such intellectual property will remain the Client's property) (together the "**ClearKey Elements**"). To the extent that any such rights may have vested in it, the Client hereby assigns to TransUnion all existing and future intellectual property rights in the ClearKey Elements and all materials embodying such rights to the fullest extent permitted by law.

4.6 The Client acknowledges that the ClearKey Service uses first party cookies (set by the Client) and third party cookies (set by TransUnion/iovation for its data capture process.

4.7 The Client shall provide (or will procure that a third party acting on its behalf will provide) Fraud Updates on a regular basis by submitting such evidence via the Intelligence Center.

4.8 The Client grants to each of TransUnion and iovation a non-exclusive, irrevocable, perpetual licence to copy, store, use and sub-licence the Input (including the internet protocol addresses that form part of the Input) and the Fraud Updates to enable TransUnion and iovation to provide services to their clients in which the Input and the Fraud Updates are used to assist with identity verification and prevention of fraud/money laundering. This paragraph 4.8 shall survive the expiry or termination of this Agreement.

4.9 The Client warrants to TransUnion that, in compliance with the Applicable Law (including the Data Protection Legislation), applicable consent has been obtained, and appropriate notices have been given to its customers, that the data relating to those data subjects may be processed in the manner described in paragraphs 4.4, 4.6 and 4.8 above. This notice shall include a link to (i) the TransUnion Bureau Privacy Notice, currently available at https://www.transunion.co.uk/legal/privacy-centre/pc-bureau, and (ii) the iovation privacy policy currently available at https://www.iovation.com/privacy, (or in either case such replacement URL as notified to the Client from time to time).

4.10 The Client acknowledges that neither TransUnion nor its subcontractor make any warranties or representations (i) as to the suitability of the ClearKey Service and ClearKey Output Data for any particular purpose; (ii) as to the accuracy or completeness of the ClearKey Output Data; or (iii) that the ClearKey Service will be uninterrupted or continuously available. For the avoidance of doubt, unless expressly stated to the contrary, all warranties provided by TransUnion as part of the General Terms are provided by TransUnion only.

4.11 The Client shall not create or attempt to create (or permit others to create or attempt to create), by reverse engineering or otherwise, the source programs or any part thereof from the object programs or from any other information made available to it by TransUnion or its subcontractor under this Agreement and shall not decompile, disassemble, modify, alter or create derivative works of the Service. Liability for a breach of this Service Condition shall be unlimited, notwithstanding the liability provisions set out in clause 10 of the General Terms.

4.12 Nothing contained in this Agreement shall be construed as granting or conferring any right, title, or interest, in any proprietary information, patent, trade mark, copyright, trade secret or other proprietary right in the ClearKey Service or Device Identifying Software that is now or subsequently owned by iovation or TransUnion.

4.13 Without prejudice to clause 5.7 of the General Terms, if the ClearKey Output Data contains a system error message, this is an indicator that either the system has timed out or that there is an internal system issue and no assumption should be made by the Client (on the basis of this error message) as to the likelihood that the device being used to access an account matches (or does not match) a device that has been registered to that account.

4.14 The Client acknowledges that iovation will provide all after sales support. The contact email for support and queries relating to the ClearKey Service (to be used instead of the email address shown in the Primary Schedule) is TruValCSupt@transunion.com.

4.15 The Client agrees that it shall only use the ClearKey Service in respect of customers who are resident in the UK, Isle of Man, the Channel Islands, the EEA or the USA.

4.16 The Client acknowledges that the ClearKey Service is not intended to be indicative of a customer's creditworthiness or eligibility for insurance. Without prejudice to paragraph 2 of this Service Schedule (Permitted Purpose) and clause 5.1.1 of the General Terms, the Client warrants that it shall not use the Output from the ClearKey Service as a factor in establishing any customer's eligibility for credit or insurance.

4.17 The Client shall not use the ClearKey Service as the sole basis for any business decision. Without prejudice to clause 8.10 of the General Terms, the Client shall not use the ClearKey Service (including any Output) to make a decision based solely on automated processing (including profiling) in relation to a data subject where such decision produces legal effects concerning that data subject or similarly significantly affects that data subject (including entirely preventing a data subject from signing up or accessing the Client's services) except where the Client is permitted to do so pursuant to the Data Protection Legislation. Where it is so permitted to make such decision, the Client shall at all times comply with all relevant requirements as set out under the Data Protection Legislation in relation to that data subject's rights and freedoms and legitimate interests in connection with that decision.

4.18 Where requested by the Client, available Transaction Insight Data will be collected and will be accessible via the Intelligence Center.

SERVICE SCHEDULE

DOCUMENT VERIFICATION FACIAL BIOMETRICS (AU10TIX) ONLINE

Commented [MS3]: This Service Schedule contains all options - the Schedule will need to be tailored to reflect the particular options and permitted purposes applicable for the relevant client at Call-Off stage. Therefore, not all provisions in this Service Schedule will be applicable at the Call-Off stage.

1. **DESCRIPTION OF THE SERVICES**

In this Service Schedule, the Services shall comprise the following:

- **Solution(s)**: Mobile SDK, Web SDK, Web App, Mobile App, Submission API;
- **Product Component(s)**: GIID Verification, Proof of Liveness and Biometric Comparison, Additional Document Processing;
- **Additional Options**: Biometric Authentication, Manual Review, SMS provision, Serial Fraud Monitor, UK Hosting;
- **Results Interface(s)**: Client Console, Post Processing Webhook, GET API;
- DVFB PoC;
- Data Storage;
- Access to Sandbox Facility;
- Pre-Sales Consultancy; and
- Maintenance and support services.

2. **PERMITTED PURPOSE**

2.1 To assist the Client with identity verification and/or anti-money laundering and/or the detection/prevention of fraud or financial crime, for the Client's internal business purposes only.

2.2 For the DVFB PoC only, to assist the Client in its assessment of the Services for the purposes of identity verification and/or anti-money laundering and/or the detection/prevention of fraud or financial crime. The Client agrees that the Output and the results of the Client's internal evaluation shall not be used by the Client in a live production environment or to build a scorecard(s). For the avoidance of doubt, unless this Service Schedule is terminated in accordance with paragraph 3.2, the permitted purpose in paragraph 2.1 shall apply on and from the day immediately following the end of the DVFB PoC.

3. **SERVICE SCHEDULE DURATION**

3.1 Insert Details (Where Applicable)As set out in the Primary ScheduleSubject to paragraph 3.2 Insert Details (Where Applicable)As set out in the Primary Schedule.

3.2 The Client is permitted to terminate this Service Schedule at any time in the first thirty (30) days after the Service Start Date by giving TransUnion not less than seven (7) days' written notice (i.e. the last day to service such notice shall be twenty-three (23) days after the Service Start Date ("**DVFB PoC Termination**"). Any purported notice of DVFB PoC Termination served after the twenty third day following the Service Start Date shall have no effect.

4. **SERVICE CONDITIONS**

These Service Conditions shall apply in respect of the Services.

4.1 In respect of these Service Conditions the following additional definitions apply:

"**Additional Document**" means an identity document that is not a GIID, and which has been photographed and/or uploaded as a pdf by the End User;

"**Additional Document Processing**" means the extraction of personal data from an Additional Document using proprietary OCR technology and, where available, a comparison of the name and address extracted with the name and address on the GIID;

"**Age Estimation**" means the optional functionality within the Proof of Liveness Product Component that provides an estimate of the End User's age based on the captured Selfie Face, which can be compared to the age calculated based on the GIID date of birth;

"**Attack**" means a combination of repetitions and conflicts identified by the Sub-processor that may indicate a synthetic identity attack;

"**Au10tix**" means Au10tix Ltd (an Israeli private company whose company number is 514553007), with address at 5B Hanagar St., Hod Hasharon, Israel;

"**Biometric Authentication**" means the Additional Option which compares a Biometric Representation derived from a Reference Facial Image with a Biometric Representation derived from a Selfie Face provided by an End User, in order for the End User to authenticate their identity;

"**Biometric Comparison**" means the Product Component which compares the Biometric Representation derived from the Document Face with the Biometric Representation derived from the Selfie Face;

"**Biometric Representation**" means a representation created through proprietary and/or licensed algorithms of the unique set of coordinates comprising a Facial Image captured through the Solutions;

"**Client Branding**" means one or more of the fonts, logos, colours, trade names or other trade marks that are owned by or licensed to the Client and/or members of its group that the parties have agreed are to be incorporated into the Solution;

"**Client Console**" means the browser-based interface which allows the Client to access the Data Storage and view the Processing Output, and to generate summary reports enabling it to meter usage and monitor performance of the Solutions and Product Components;

"**Client Console Users**" means those Client Users who are authorised (have been given unique user credentials) to access the Client Console;

"**Client User Data**" means any data relating to a Client User that is provided to TransUnion or the Sub-processor to enable the Client User to access the Services (including the Client Console and the TransUnion Client Service Desk);

"**Client Users**" means those members of the Client's staff who are users of the Services;

"**Closed Garden**" means, for the purposes of the Serial Fraud Monitor Service, the configuration of the Shared Consortium Database which contains Processing Output contributed by the Client only;

"**Data Storage**" means the backend database, hosted by the Sub-processor, which contains (subject to the Client's requirements in relation to data retention referred to in paragraph H of Annex 1) all of the Processing Output and which may, dependent on the Solution taken and the Client requirements, be accessed via the Results Interfaces;

"**Device Environment Attributes**" means information that may be captured or accessed by the Sub-processor using cookies or similar technologies placed on an End User's device in order to facilitate the operation of the Solution components;

"**Document Face**" means the Facial Image contained in a GIID, either on the face of the GIID or within the NFC Chip (where available);

"**Documentation**" means the Sub-processor's instructions, guides (including technical guides) and manuals made available to the Client by TransUnion, any drawings, diagrams, designs, pictures or other images, tapes, disks or other devices or records embodying information in any form as published by TransUnion and/or the Sub-processor and/or made generally available by TransUnion and/or the Sub-processor in relation to the use of the Services and/or sales and marketing materials;

"**DVFB**" means Document Verification and Facial Biometrics;

"**DVFB PoC**" means the programme lasting 30 days and commencing on and from the date of the first Test Transaction, which allows the Client to trial the Services (including the Solutions, Product Components, Additional Options (but not Manual Review or UK Hosting) and Results Interfaces specified in paragraph 1) using the Sandbox Facility subject to the permitted purpose set out in paragraph 2.2 and the restrictions set out in

paragraph 4.4.3;
"**End User**" means a customer or potential customer of the Client's products/services who is a user of the Solution;
"**Facial Image**" means an image of a natural person that may be used for the purposes of allowing or confirming the unique identification of that person;
"**Geolocation Data**" means the geographical location information (in longitude and latitude format) that is collected from an End User's device using where enabled and consented to by the End User;
"**GET API**" means the Results Interface that allows the Client to electronically retrieve the Processing Output from the Data Storage;
"**GIID**" means a Government-issued ID document, which includes a Facial Image;
"**GIID Verification**" means the Product Component which analyses a GIID in order to ascertain its authenticity and validity;
"**Good Industry Practice**" means the exercise of that degree of skill, diligence, prudence and foresight which would ordinarily be expected from a skilled and experienced operator engaged in providing services of the same kind as the Services seeking to comply with its contractual obligations and all Laws relating to the Services;
"**GPS**" means Global Positioning System and is a device feature that uses satellite data to calculate the geographical position of the device;
"**Infringement Claim**" includes any claim by a third party that use of the Services, Solutions, Software or Documentation infringes, allegedly infringes, violates or constitutes a wrongful use of any third party's IPR or other proprietary rights of any person;
"**Intellectual Property Rights**" or "**IPR**" means all forms of intellectual property rights and protections throughout the world, including, but not limited to, any (a) patents (including any patent applications, together with all reissuances, continuations, continuations-in-part, revisions, extensions and re-examinations thereof); (b) copyrights; (c) internet domain names, trade marks, service marks, and trade dress, together with all goodwill associated therewith; (d) trade secrets; (e) rights in databases and designs (ornamental or otherwise); (f) moral rights, rights of privacy, rights of publicity and similar rights; and (g) any other proprietary rights and protections, whether currently existing or hereafter developed or acquired, whether published or unpublished, arising under statutory law, common law, or by contract, and whether or not perfected, including all applications, disclosures and registrations with respect thereto;
"**Malicious Code**" means any "virus" or "worm", "Trojan Horse", "trapdoor", "Software Switch", "time bomb" or "logic bomb", "disabling code" or "disabling routines", "expiration dates", "protect codes", "data destruct keys", "worms", and other harmful or malicious code, files, scripts, agents, or programs;
"**Manual Review**" means the manual review of information submitted by the relevant Solutions where the Product Components selected have not been able to provide a conclusive result;
"**Mobile App**" means the mobile application which operates on mobile devices running iOS and Android operating systems;
"**Mobile SDK**" means the software development kit that assists the Client in building a DVFB mobile application for iOS and/or Android platforms. It enables the Product Components to be presented to End Users, via incorporation into the Client's own mobile app;
"**NFC Chip**" means the Near Field Communication chip embedded in some GIIDs containing the personal information printed on the GIID in addition to an electronically encoded copy of the photograph of the GIID holder that was supplied at the point of issue of the GIID, which can be used to assist in the authentication of the identity of the GIID holder;
"**OCR Data Extraction**" means the extraction of data via the application of proprietary optical character recognition technology;
"**PECR**" means the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended from time to time;
"**Post Processing Webhook**" means the facility for the Client to electronically receive the Processing Output direct from the Data Storage;
"**Pre-Sales Consultancy**" means the consultancy work undertaken by TransUnion and/or the Sub-processor in exploring the Client's requirements and Solution options;
"**Processing Input**" as defined in the Data Processing Annex;
"**Processing Output**" as defined in the Data Processing Annex;
"**Proof of Liveness**" means the Product Component which assists in determining whether the Facial Image captured by the Solution is from a live individual or is an image or video displayed on a video screen and can, if enabled, provide an Age Estimation;
"**Reference Facial Image**" means the Selfie Face provided by the End User and held by the Client for the purposes of Biometric Authentication;
"**Sandbox Facility**" means the environment hosted by the Sub-processor which allows the Client to test out Solutions, Product Components (but not Manual Review), Results Interfaces and some Additional Options based upon the Client requirements;
"**Selfie Face**" means the Facial Image that appears in a photograph taken by the End User of themself and used as part of the Transactional Processing for Biometric Authentication and/or Proof of Liveness and/or Biometric Comparison Product Component(s);
"**Serial Fraud Monitor**" means the Additional Option which assists the Client in identifying potential fraud and/or an Attack by comparing the Processing Input from the current Transactional Processing with Processing Output already stored in the Shared Consortium Database Closed Garden;
"Service Improvement" means the ongoing enhancement of algorithms, investigation of bugs and development of the Services;
"**Service Start Date**" means, for the purposes of this Service Schedule, the date of the first Test Transaction;
"**Shared Consortium Database**" means the database held by the Sub-processor which stores Processing Output from all of the Sub-processor's clients who have agreed to share data on a reciprocal basis for the purposes of the Serial Fraud Monitor Service and is used to provide the Serial Fraud Monitor Additional Option to such clients;
"**SMS Provision**" means the making available via SMS of a URL link that directs the End User to the start of an ID verification journey;
"**Software**" means the Sub-processor's proprietary software including front end and back end facilitating authentication and KYC back-office solutions, developed by the Sub-processor and provided to the Client in a consumption based 'software as a service' model including all IPR related thereto, including the Mobile SDK and Web SDK, as further detailed in this Service Schedule;
"**Submission API**" means a set of application programming interfaces (APIs) made available to the Client to enable it to submit Processing Input to the Sub-processor for Transactional Processing;
"**Test Transaction**" means the submission of Processing Input for Transactional Processing in the Sandbox Facility;
"**Transaction**" means a completed End User journey where the End User has completed the Transactional Processing without error and the results have been delivered via the Results Interface. For the avoidance of doubt, a Transaction is completed regardless of a pass/fail result;
"**Transactional Processing**" means the capture of the Processing Input by the Solution and subsequent processing by the Product Components and where applicable the Additional Options, as further detailed in paragraph C(ii) of Annex 1;
"**TransUnion Client Service Desk**" which may be contacted via email at: clientservicedesk@transunion.co.uk or by telephone on 0845 120 1222;
"**Update**" means if applicable to the Software, Documentation and/or Services, any update, patch, bug fix or incremental release(s) of the Software provided by TransUnion or the Sub-processor, including any major releases or modifications that have been made to the Software, Documentation or Services;
"**Web App**" means browser-based software delivered by the Sub-processor;
"**Web SDK**" means the software development kit used to build the web browser applications, which enables the Product Components to be presented to End Users, via the Client's own website.

4.2 The Sub-processor

4.2.1 TransUnion has appointed Au10tix as its sub-processor in relation to the Services and, for the purposes of Article 28(2) of the GDPR, hereby gives its specific written authorisation to TransUnion to use Au10tix as its processor (the "**Sub-processor**").

4.2.2 As a result of TransUnion's reliance on the Sub-processor for the delivery of the Services, clause 14.1 of the General Terms shall be extended to cover an Event of Force Majeure suffered by the Sub-processor. In such circumstances, TransUnion shall procure that the Sub-processor shall comply with the provisions of clause 14.2 and in the event that TransUnion is unable to perform its obligations under this Service Schedule by reason of the Sub-processor's Event of Force Majeure for a period of more than four weeks, TransUnion may terminate this Service Schedule immediately by serving notice on the Client and shall not be liable to the Client by reason of such termination.

4.3 Implementation Plan

4.3.1 A meeting (or meetings) shall be held between the parties prior to Services Commencement, during which an implementation plan and schedule of works (the "**Implementation Plan**") will be discussed and agreed.

4.3.2 To the extent that the Client wishes to make any amendments after the parties have agreed the Implementation Plan, TransUnion reserves the right to charge an additional fee in respect of professional service hours that will be incurred. Where TransUnion intends to invoke this right, it shall give notice to the Client of the estimated professional service hours and related fee before implementing the requested changes.

4.3.3 The Client shall at all times co-operate with TransUnion and provide TransUnion and/or the Sub-processor with such information and assistance as TransUnion may reasonably require in order to enable TransUnion and the Sub-processor duly and punctually to perform to meet the Implementation Plan.

4.4 Sandbox Testing

4.4.1 In order to test out the Solutions, Product Components (excluding Manual Review) and Results Interfaces, the Sub-processor shall make available to the Client the Sandbox Facility.

4.4.2 The Client is permitted to perform Transactional Processing through the Sandbox Facility, undertaking up to 1000 Test Transactions over a maximum period of 30 days commencing with the first Test Transaction.

4.4.3 For the avoidance of doubt, where the Client uses the Sandbox Facility for the purposes of a DVFB PoC, and the Client wishes to add to or amend any of the Solutions, Product Components, Additional Options and/or Results Interfaces specified in paragraph 1, then the Client shall terminate this Service Schedule in accordance with paragraph 3.2 or enter into a letter of variation to amend this Service Schedule to properly reflect the Services to be taken on an ongoing basis.

4.5 Device Environment Attributes

4.5.1 Collection of Device Environment Attributes involves the placing of cookies or similar technologies on the End User's device. The Client warrants to TransUnion that, in compliance with the Applicable Law (including PECR), all appropriate notices have been given and applicable consents have been obtained to enable the setting and reading of such cookies.

4.5.2 Unless the GPS feature in an End User's mobile device has been switched off or the device does not have access to GPS, Geolocation Data will be captured as part of the Device Metadata.

4.6 Solutions and Product Components

4.6.1 The Mobile SDK Solution may only be utilised for transmitting the Processing Input to the Sub-processor and applicable Additional Options for Transactional Processing and expressly excludes the transmission of Processing Input to any other provider of services equivalent to the Services described in this Service Schedule.

4.6.2 Where the Client opts to enable the Age Estimation feature in the Proof of Liveness Product Component, the Client agrees that it shall not make a determination of fraud based solely on the age estimate provided by this feature.

4.6.3 The Client acknowledges that Additional Document Processing does not provide an assessment of the validity and authenticity of the Additional Document.

4.6.4 The Client acknowledges that the implementation and operation of the Biometric Authentication Additional Option is dependent on the Client requiring the End User to provide a photograph of the End User, which the Client has stored on its own system and the End User consenting to this.

4.6.5 For Serial Fraud Monitor, the Client agrees to the storage of its Processing Output in the Fraud Consortium Database and the use of such Processing Output to enable TransUnion or its Sub-processor to provide the Serial Fraud Monitor service to clients who have also opted in to the Shared Consortium Database. The Client grants to TransUnion and its Sub-processor a non-exclusive, royalty free licence to use the Processing Output in this way and shall take all steps necessary to ensure that End User's personal data can be shared and stored in this manner and for this purpose. For the avoidance of doubt, save for the unique transaction ID returned in respect of any conflicting data, the Processing Output itself is not shared with other clients of TransUnion or its Sub-processor.

4.6.6 Some of the Services involve the processing of biometric data for the purpose of uniquely identifying a natural person, which is a special category of personal data under the GDPR.

4.6.7 The Client warrants to TransUnion that, in compliance with the Applicable Law (including Data Protection Legislation), consent has been obtained by the Client, and appropriate notices have been given to End Users, to enable the data provided by the End Users to be processed in the manner described in this Service Schedule and the Data Processing Annex.

4.6.8 The Client shall not oblige End Users to use the DVFB Services for the purposes of identity verification and shall offer alternative methods by which an End User can verify their identity and/or have their documents validated and shall not discriminate against an End User because of their refusal to agree to use electronic identity or document verification systems.

4.6.9 The Client acknowledges that delivery of the Services may be subject to specific technological requirements published by the Sub-processor from time to time (a copy of which is available on request), including any hardware or software required at the Client's site in order to install and use the Services. Any such technological requirement shall be procured by the Client at its cost and under its sole responsibility as a condition precedent to the provision of the Services.

4.6.10 TransUnion warrants that the Services shall be free from material defects. However, the following are excluded from such warranty:

4.6.10.1 defects discovered in any component of the Service that has been modified, altered, or enhanced without TransUnion's prior written consent;

4.6.10.2 defects resulting from or occurring from any act or omission not taken by TransUnion or the Sub-processor;

4.6.10.3 defects due to the Client's system; or

4.6.10.4 any defects arising from the use of the Services otherwise than in accordance with the terms and conditions of this Agreement & Service Schedule.

4.6.11 Without prejudice to clause 8.12 of the General Terms, the Client shall not use the Services (including the Processing Output) to make a decision based solely on automated processing (including profiling) in relation to a data subject where such decision produces legal effects concerning that data subject or similarly significantly affects that data subject except where the Client is permitted to do so pursuant to the Data Protection Legislation. Where it is so permitted to make such decision, the Client shall at all times comply with all relevant requirements as set out under the Data Protection Legislation in relation to that data subject's rights and freedoms and legitimate interests in connection with that decision.

4.7 Operation of the Results Interfaces

4.7.1 The Client shall provide a secure web listener URL in order to receive the Processing Output via the Post Processing Webhook.
4.7.2 The Client shall ensure that the Post Processing Webhook includes the same unique identifier that was included in the Processing Input in order to match to the specified transaction.
4.7.3 The Client shall ensure that the request to the GET API includes the same unique identifier that was included in the Processing Input in order to match to the specified transaction.
4.7.4 The Client shall ensure that each Client Console User keeps their user credentials for access to the Client Console confidential. User credentials shall not be shared between individuals and, where abuse is suspected, TransUnion reserves the right to suspend the account pending an investigation.
4.7.5 The Client acknowledges that data provided to the Client via the Results Interfaces may not contain all the personal data held in the Data Storage Facility and that, in order to comply with a data subject access request under the GDPR, the Client will need to make a Processor Request under paragraph 4.12.6.
4.8 Service Improvement
4.8.1 The Client agrees that the Sub-processor may retain 1% of the Processing Output for Service Improvement, including the ongoing enhancement of algorithms and investigation of bugs.
4.8.2 For the avoidance of doubt, notwithstanding the Client's agreement to permit this Processing Output to be retained for Service Improvement, the Sub-processor shall continue to own all intellectual property rights in any resulting algorithms, Software or Updates (together "the Updated Materials"). To the extent that any such rights may have vested in it, the Client hereby assigns to TransUnion on behalf of the Sub-processor all existing and future intellectual IPR in the Updated Materials to the fullest extent permitted by law.

4.9 Intellectual Property
4.9.1 Without prejudice to clause 6.2 of the General Terms, any intellectual property rights in the Client Branding shall at all times remain vested in the Client (or its third party licensors) and neither TransUnion nor the Sub-processor shall acquire any rights in them save as expressly provided in this Service Schedule.
4.9.2 The Client grants to TransUnion and the Sub-processor a non-exclusive, royalty-free licence for the term of this Service Schedule to use the Client Branding solely for inclusion in the Solutions (where relevant) and/or to the extent necessary for TransUnion to provide the Services described in this Service Schedule.
4.9.3 Subject to the license rights as set out herein, as between the TransUnion and the Client, all right, title, and interest in and to the Services, Software, Updates, TransUnion's or the Sub-processor's Confidential Information, and Documentation, excluding any Processing Input and Processing Output, including, without limitation, all modifications, derivative works, enhancements, and IPR therein and thereto, shall belong solely to TransUnion and/or its applicable licensors. To the extent that the Client, by operation of law, is deemed to have any rights in or to the software, updates, TransUnion's or the Sub-processor's Confidential Information, or Documentation, the Client shall, and hereby does, exclusively and irrevocably assign, transfer and otherwise convey to the TransUnion all of its right, title, and interest in and to the Services, Software, Updates, TransUnion's or the Sub-processor's Confidential Information, or Documentation (excluding Processing Input and Processing Output), including without limitation all IPR pertaining thereto.
4.9.4 TransUnion grants to the Client a non-transferable, revocable, non-exclusive, non-sublicensable licence to use and copy the Intellectual Property Rights of TransUnion or its third-party licensors contained in the Services strictly only for the purpose of exercising the Client's rights and performing its obligations under this Service Schedule. All rights not expressly granted to the Client are reserved by the Sub-processor and its licensors. The Au10tix name, the Au10tix logo and the certain product names associated with the Service are trade marks of the Sub-processor, TransUnion or third parties, and no right or license is granted to use them. The Sub-processor's trade marks are set out via a link on the Sub-processor's website that TransUnion shall make available to the Client on request.
4.9.5 The Client shall not knowingly:
4.9.5.1 use the Services to store or transmit infringing, libellous or otherwise unlawful or tortious material, or to store or transmit in violation of third-party rights;
4.9.5.2 interfere with or disrupt the integrity or performance of the Services; or
4.9.5.3 attempt to gain unauthorised access to the Services or the Sub-processor's related systems or networks.
4.9.6 The Client shall not:
4.9.6.1 alter, modify, translate, reproduce or create derivative works of the Services, or any part thereof;
4.9.6.2 attempt to derive the source code of the Services, reverse engineer, decompile or disassemble the Services or otherwise reduce the software embodied therein to human-perceivable form, or encourage or assist third parties in doing so.
4.9.7 For the avoidance of doubt, neither TransUnion (nor the Sub-processor) shall be liable for any Infringement Claim to the extent that such liability is based upon or arising from (a) use of the Services in a manner not in accordance with the Documentation, (b) modifications to the Services by anyone other than TransUnion or the Sub-processor; (c) connection or combination of a Service with any third party software or hardware not approved in writing by TransUnion or the Sub-processor where such connection or combination is the sole cause of an infringement, or where such liability is directly the result of the Client's (or any End User's) continued use of an infringing version of the Services when the current version of the Services has been modified to be non-infringing and TransUnion has provided the Client with such non-infringing version in accordance with clause 3.2 of the General Terms.

4.10 Other obligations and acknowledgements of the Client
4.10.1 Subject to paragraph 4.10.2, TransUnion acts solely as processor on behalf of the Client in respect of the processing of personal data contained within the Processing Input and the Processing Output. The Client is the controller in respect of such personal data.
4.10.2 TransUnion acts as a controller in respect of any personal data contained within the Client User Data held by or on behalf of TransUnion. TransUnion shall and shall procure that the Sub-processor shall process such personal data in accordance with the notice displayed on the TransUnion website, at such URL as is notified to the Client from time to time.
4.10.3 The Client agrees that, where TransUnion is acting as processor, then paragraph 4.12 of these Service Conditions shall apply.
4.10.4 Without prejudice to clause 10.3 of the General Terms, TransUnion makes no representations as to the suitability of the Services for the purposes of compliance with any legislation or regulation. The Client is responsible for satisfying itself that the Processing Output meets any such requirement.
4.10.5 TransUnion is the first line of support, and the Client agrees that it will request assistance from TransUnion in respect of any maintenance and support issues that arise in relation to the Services. The Client further agrees that it will not contact the Sub-processor directly except with the prior agreement of TransUnion.
4.10.6 TransUnion shall provide the Services in accordance with the applicable service levels set out in the Service Level Schedule attached to this Service Schedule (subject to the requirement that the Client complies with its obligations under the Service Level Schedule). The sole and exclusive remedy of the Client for any breach of this provision shall be the service credits system under the Service Level Schedule.
4.10.7 The Client warrants that it will apply standards and controls in accordance with Good Industry Practice to try to prevent transmission to TransUnion or the Sub-processor of any Malicious Code.

4.10.8 The Client agrees that it shall only use the DVFB Services in respect of customers who are resident in the UK, Isle of Man or the Channel Islands.

4.11 Disclaimer of warranties

4.11.1 The Service and all content are provided to the Client strictly on an "as is" and "as available" basis. To the maximum extent applicable by law, TransUnion, the Sub-processor, and its licensors make no other representation, warranty (whether statutory, express, implied or otherwise) or guarantee as to the availability, timeliness, truth, accuracy, reliability, suitability, merchantability, completeness or non-infringement of the Service or any content except as expressly stated in this Service Schedule (including, for the avoidance of doubt, the Service Level Schedule). Without derogating from the generality of the foregoing and except as expressly stated in this Agreement, TransUnion does not represent or warrant that: (a) the use of the Service will be timely, uninterrupted, error-free or operate in combination with any other hardware, software, system or data; (b) the Service will be of satisfactory quality, performance or accuracy; or (c) the Service will meet the Client's requirements or expectations.

4.11.2 The Service may be subject to limitations, delays and other problems inherent in the use of the internet and electronic communications. TransUnion accepts no responsibility for any delays, delivery failures, or other damage resulting from such problems to the extent caused by the Client's equipment, systems or internet or electronics communications provider(s).

4.11.3 For the avoidance of doubt, and to the maximum extent permitted by law, except for any warranties expressly stated in this Agreement, the entire risk arising out of the Client's use of the Services remains with the Client.

4.12 Data Processor obligations

4.12.1 This Service Condition 4.12 only applies in relation to any personal data in the Processing Input and Processing Output and, for the purposes of this Service Schedule only, shall take precedence over clause 8 of the General Terms in the event of any inconsistency.

4.12.2 The parties acknowledge and agree that their respective statuses as controller or processor for the purposes of this Service Schedule are as set out in paragraph 4.10.1 and 4.10.3.

4.12.3 To the extent that TransUnion is acting as a processor of personal data on behalf of the Client in respect of this Service Schedule, it shall:

4.12.3.1 implement appropriate technical and organisational measures in such a manner that its processing of the personal data will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the relevant data subjects;

4.12.3.2 not engage another processor of the personal data without prior specific or general written authorisation of the controller and, where it relies on a general authorisation, inform the controller of any intended changes concerning the addition or replacement of other processors;

4.12.3.3 where it engages another processor for carrying out processing activities on behalf of the Client, impose obligations on that other processor that are substantially equivalent to the terms set out in this paragraph 4.12.3;

4.12.3.4 process the personal data only on documented instructions from the Client or as otherwise required by Applicable Law;

4.12.3.5 not transfer the personal data to an international organisation or to a place outside [both the United Kingdom and the European Economic Area] [the United Kingdom] other than on the documented instructions of the Client;

4.12.3.6 where processing personal data otherwise than on the basis of documented instructions from the Client, first inform the Client of the requirement to process it on grounds of Applicable Law, unless prohibited from doing so by Applicable Law;

4.12.3.7 ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

4.12.3.8 taking into account the nature of the processing, assist the Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests under the Data Protection Legislation in relation to the data subjects' rights of access to personal data, rectification of personal data, erasure of personal data, restriction of personal data, data portability, objection to processing of personal data, and in relation to automated individual decision-making. Any such assistance shall be requested by the Client as a Processor Request in accordance with clause 4.12.6;

4.12.3.9 notify the Client without undue delay after becoming aware of a personal data breach affecting the data being processed;

4.12.3.10 taking into account the nature of the processing and the information available to the processor, assist the Client in ensuring compliance with its obligations under the Data Protection Legislation in relation to security of processing, notification of personal data breaches to regulatory authorities and to data subjects, and carrying out and consulting with regulatory authorities in relation to data protection impact assessments. Any such assistance shall be requested by the Client as a Processor Request in accordance with clause 4.12.6;

4.12.3.11 at the choice of the Client, delete or return the personal data to the Client after the end of the provision of the Services, and delete existing copies unless required to store it by Applicable Law;

4.12.3.12 make available to the Client all information necessary to demonstrate compliance with the obligations under the Data Protection Legislation in relation to the appointment and use of processors;

4.12.3.13 allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client, in accordance with clause 13 (Audit) of the General Terms; and

4.12.3.14 immediately inform the Client if, in its opinion, an instruction given by the Client infringes the Data Protection Legislation or any other Applicable Law relating to data protection.

4.12.4 For the purposes of paragraph 4.12.3.2:

4.12.4.1 the Client hereby gives TransUnion a general authorisation to appoint any other processor to process the Input and the Output in accordance with this Agreement;

4.12.4.2 if the Client objects to the appointment of a processor, the parties shall enter into good faith negotiations, during which time TransUnion may suspend the supply of the Services, with a view to agreeing an alternative processor acceptable to the Client and a variation to the Fees reflecting any consequential increase in TransUnion's costs; and

4.12.4.3 if the parties fail to reach an agreement under 4.12.4.2 within a period of 14 days, TransUnion may by written notice immediately terminate this Service Schedule (including all licences granted under it).

4.12.5 For the purposes of paragraphs 4.12.3.4, and 4.11.3, the terms of this Agreement (including the contents of the Data Processing Annex) are deemed to be documented instructions of the Client.

4.12.6 Where the Client wishes to make a change to the Services (including the documented instructions) or request assistance under paragraph 4.12.3.8 or 4.12.3.10, the Client shall notify TransUnion in writing (a "**Processor Request**").

4.12.7 As soon as practicable after receipt of the Processor Request, TransUnion shall specify whether it is able to effect the change/provide the requested assistance and if so what additional charge (if any) shall be levied on the Client.

4.12.8 Any Processor Request (and the appropriate charge to be levied) shall be agreed in writing between the parties and signed by appropriately authorised representatives.

4.12.9 Nothing in this Agreement shall relieve TransUnion of its own direct responsibilities and liabilities as a processor under the Data Protection Legislation.

4.13 Data Retention Instructions

4.13.1 TransUnion shall procure that the Sub-processor shall delete the data contained in the Test Transactions, including Device Environment Attributes, at the end of [INSERT NUMBER] [INSERT UNIT] from the date/time the Test Transaction was undertaken.

4.13.2 TransUnion shall procure that the Sub-processor shall delete the Processing Input and Processing Output, including Device Environment Attributes, at the end of [INSERT NUMBER] [INSERT UNIT] from the date/time the Processing Input was received.

4.13.3 TransUnion shall procure that the Sub-processor shall delete the End User Communications Data at the end of [INSERT NUMBER] [INSERT UNIT] from the date/time such data was received by the Sub-processor.

4.13.4 TransUnion shall procure that the Sub-processor shall delete the data contributed to the Shared Consortium Database Closed Garden at the end of 35 days from the date/time it was first contributed save where such data has been tagged as Attack Data in which case the end of 2 years from the date/time it was first contributed.

4.13.5 TransUnion shall procure that the Sub-processor shall delete the data retained by the Sub-processor for Service Improvement, including Device Environment Attributes, at the end of [INSERT NUMBER & UNIT] from the date/time the Processing Input was received.

ANNEX 1 – DATA PROCESSING
DOCUMENT VERIFICATION FACIAL BIOMETRICS (AU10TIX)

This Data Processing Annex records certain details concerning the processing to be performed by TransUnion acting as a processor of personal data (and by Au10tix as its sub-processor) on behalf of the Client pursuant to this Service Schedule. TransUnion may give notice to the Client of changes to the Data Processing Annex from time to time but only to the extent necessary to comply with record keeping obligations under the Data Protection Legislation.

Identity of the processor(s) and controller

Processor:	TransUnion International UK Limited (company number 03961870), registered office: One Park Lane, Leeds, West Yorkshire LS3 1EP
Approved sub-processors:	Au10tix Ltd, 5B Hanagar St., Hod Hasharon, Israel Au10tix may also use other sub-processors to fulfil the Services; a full list shall be provided to the Client upon request.
Controller:	[INSERT DETAILS OF CLIENT LEGAL ENTITY]

A. Subject matter of the processing
DVFB involves TransUnion's Sub-processor performing identity verification and fraud prevention services on behalf of the Client through review and analysis of End Users' GIIDs and, where selected, comparison of GIIDs with End Users' 'selfie' photographs and liveness checks through such 'selfie' photographs. Additionally, TransUnion's Sub-processor may compare GIIDs with stored GIID information to identify potential fraud and/or involvement of the GIID in an Attack.

B. Duration of the processing
As set out in paragraph 3 of this Service Schedule (Service Schedule Duration), subject to earlier deletion of the data in accordance with paragraph H below.

C. Nature and purpose of the processing
TransUnion will process End Users' personal data as necessary to perform the Services described in this Service Schedule.

(i) SMS provision
- use and storage of End User mobile telephone numbers ("**End User Communications Data**")
  Purpose: to contact the End User in order to start the ID verification journey and/or for Biometric Authentication.

(ii) GIID Verification:
- OCR Data Extraction
- (where appropriate) reading of the eChip from the GIID
- (where appropriate) use of cookies or similar technologies to extract Device Environment Attributes
- (where appropriate and switched on by the End User) collection of Geolocation Data
- proprietary assessment of the End User's GIID to identify potential anomalies

Proof of Liveness:
- proprietary assessment of liveness of the captured Selfie Face
- (where enabled) proprietary estimation of age based on the captured Selfie Face

Biometric Comparison:
- biometric comparison of the captured Selfie Face and Document Face

Additional Document Processing:
- capture of Additional Document and OCR Extraction
- where available, name and address matching with GIID
  Purpose: to enable Processing Output to be created.

(iii) Biometric Authentication
- comparison of a Biometric Representation derived from a Selfie Face uploaded by the End User with a Biometric Representation derived from that End User's Selfie Face stored by and submitted by the Client.
  Purpose: to authenticate an End User's identity

(iv) Serial Fraud Monitor
- OCR data extraction
- (where appropriate and switched on by the End User) collection of Geolocation Data
- pseudonymisation of all data using a one-way hash algorithm
- analysis and comparison with previously hashed stored data
- storage of hashed data in within the Fraud Consortium Database or Closed Garden
  Purpose: to help identify potential fraudulent activity and/or involvement of the GIID in an Attack

(v) Results Interfaces and Data Storage:
- sorting, saving and storage of the Processing Input and Processing Output
- Client access to the Processing Output via the Client Console (where appropriate)
- retrieval of Processing Output by the Client using the GET API (where appropriate)
- receipt of Processing Output via the Post Processing Webhook (where appropriate)
- deletion of data in accordance with Client instructions (see paragraph H below)
  Purpose: to enable access and for record-keeping purposes

(vi) Service Improvement (where agreed to by the Client)

- collection of 1% of Processing Output ("**Fractional Data**")
- storage of the Fractional Data
- analysis of Fractional Data
- use of aggregated Fractional Data for Service Improvement (including investigating bugs and improving algorithms)
  Purpose: to improve Service effectiveness

D. Types of personal data

(i) **Processing Input**

- GIID image
- Data extracted from the GIID including name, address, date of birth, gender, nationality, document type, ID number(s), date of issue, date of expiry, issuing authority, place of issue, Document Face and image of the signature
- Where available and enabled on a device, this may also include data extracted from the NFC Chip (not available with Submission API)
- Where the Mobile SDK Solution is taken, Device Environment Attributes
- Where the Web SDK Solution is taken, Device Environment Attributes
- Where Proof of Liveness, Biometric Comparison and/or Biometric Authentication is undertaken, a Selfie Face
- Where Additional Document Processing is taken, an image of the Additional Document and data extracted from it, primarily name and address
- Where the SMS Provision is taken, this may include End User mobile phone numbers and/or other unique identifiers

(ii) **Processing Output**

- Date and time stamp of the processing of the data
- Unique transaction ID
- Copy of the GIID image
- Information extracted from the face of the GIID as described in (i) above
- Information extracted from the NFC Chip, where relevant (not available with Submission API)
- Electronic image of the signature extracted from the GIID
- Age calculation
- Age Estimation result (where Proof of Liveness is taken, and feature has been enabled)
- Document Face
- Where Additional Document Processing is taken, an image of the Additional Document, information derived from OCR Data Extraction and, where available, the result of any name and address matching
- Where Serial Fraud Monitor is taken: a flag indicating where a duplicate is identified with a count of duplicates for each data element; a flag indicating that a conflict has been found, the type of test that detected it (e.g. seen that photo, seen that number, etc) and the unique transaction ID for the conflicting data; and a flag indicating that the Processing Input has been used in an Attack, with a an indication of the magnitude and severity of such Attack (RAG status). For the avoidance of doubt, the duplicate and/or conflicting data itself is not presented as Processing Output
- Processing results including verification results, scores, status codes, error codes and fraud codes/types where applicable and decisioning data as described in the Documentation

(iii) **Special Category Data**

Where Proof of Liveness and/or Biometric Comparison and/or Biometric Authentication are taken, biometric data is processed in the form of a Biometric Representation of the Facial Images presented through the GIID and the Selfie Face.

(iv) **Identifiers**

The personal data processed will also include a:

- Client identifier for each End User; and a
- Sub-processor identifier for each End User.

E. Categories of data subject

End Users who wish to purchase or consume products/services provided by the Client.

F. Security of processing

As set out in clause 8.11 and as further detailed within TransUnion's information security policies from time to time.

G. Transfers of personal data outside the UK or EEA

Where the Client has not selected UK Hosting, personal data is hosted (processed and stored) in the Netherlands for the purposes of Transactional Processing.

Where the Client has selected UK Hosting, personal data is hosted (processed and stored) in the United Kingdom for the purposes of Transactional Processing.

Additionally, irrespective of the Client's selection of UK Hosting:

- for Product Support purposes, End User personal data is viewed, stored, or processed in Israel,
- for content-based firewall and content delivery network services, an End User's IP address is processed and stored in the USA,
- for authentication purposes, a Client User's personal data is processed and stored in the USA,
- if the Client permits the use of its data for Service Improvement purposes, End User personal data is viewed, stored, or processed in Israel,
- if the Client has selected Manual Review, End User personal data is processed in the Philippines and stored/backed up in the USA,
- if the Client has selected Additional Document Processing, End User personal data is processed and stored in the USA and may be processed in Luxembourg,
- if the Client has selected SMS Provision, and opted to use the Sub-processor to send out the SMSs, End User personal data is processed in the USA, and
- if the Client has selected Serial Fraud Monitor, End User personal data is processed in Dublin, the Netherlands, Japan and the USA.

H. Ongoing data retention and deletion

In accordance with the Client's documented instructions (as set out in paragraph 4.13 of this Service Schedule) ("**Data Retention Instructions**")

I. Data retention or deletion upon completion of Services
On termination of this Service Schedule, TransUnion shall procure that the Sub-processor shall, unless prohibited from doing so by law, securely delete or destroy any remaining personal data contained relating to the Services in its possession or control.

J. Data Protection Officer details
Processor:
Rosie Horsewood, Legal Director
TransUnion Information Group, One Park Lane, Leeds, West Yorkshire, LS3 1EP
Email: dpo@transunion.co.uk
Sub-processor:
Name: Dan Or-Hof
Address: 5B Hanagar St., Hod Hasharon, Israel
Email: DPO@au10tix.com

ANNEX 2 – SERVICE LEVEL SCHEDULE
DOCUMENT VERIFICATION FACIAL BIOMETRICS (AU10TIX)

[INSERT]

SERVICE SCHEDULE

DOCUMENT VERIFICATION FACIAL BIOMETRICS DEMO SOLUTION (AU10TIX)

Commented [MS4]: This Service Schedule contains all options - the Schedule will need to be tailored to reflect the particular options and permitted purposes applicable for the relevant client at Call-Off stage. Therefore, not all provisions in this Service Schedule will be applicable at the Call-Off stage.

1. **DESCRIPTION OF THE SERVICES**

In this Service Schedule, the Services shall comprise the following:

1.1 Use of a stand-alone web application ("**Demo Solution**") which demonstrates how the Product Components, Additional Options & Results Interface will function, and which can be accessed via desktop or mobile devices.

1.2 **Product Component(s)**: [GIID Verification/ Proof of Liveness and Biometric Comparison/ Additional Document Processing].

1.3 **Additional Options**: Serial Fraud Monitor.

1.4 **Results Interface**: Client Console.

1.5 Support services.

2. **PERMITTED PURPOSE**

2.1 For the Client's own internal evaluation purposes solely to assist the Client to decide whether or not to enter into contract(s) with TransUnion for TransUnion's services. For the avoidance of doubt, the Services shall not be used by the Client in a live production environment or to build scorecard(s) or form strategies of any kind or to make any decisions relating to individuals.

3. **SERVICE SCHEDULE DURATION**

3.1 This Service Schedule shall commence on the Agreement Signature Datedate of the signature of Letter of Variation NUMBER entered into between the parties ("**DVFB Demo Start Date**").

3.2 Subject to paragraph 3.3, this Service Schedule shall continue in effect for a period of thirty (30) days from the date of the first Test Transaction, at the end of which it shall automatically terminate.

3.3 In the event that no Test Transaction has been carried out before the expiry of four (4) months' from the DVFB Demo Start Date ("**Long Stop Date**"), this Service Schedule shall automatically terminate on the Long Stop Date.

4. **SERVICE CONDITIONS**

These Service Conditions shall apply in respect of the Services only.

4.1 In respect of these Service Conditions the following additional definitions apply:

"**Access Link**" means a link or QR code sent in an email or SMS generated by a Client User from the Client Console;

"**Additional Document**" means an identity document that is not a GIID, and which has been photographed and/or uploaded to the Demo Solution as a pdf by the Demo User;

"**Additional Document Processing**" means the extraction of personal data from an Additional Document using proprietary OCR technology and, where available, a comparison of the name and address extracted with the name and address on the GIID. For the avoidance of doubt, Additional Document Processing does not provide an assessment of the validity and authenticity of the Additional Document;

"**Age Estimation**" means the optional functionality within the Proof of Liveness Product Component that provides an estimate of the Demo User's age based on the captured Selfie Face, which can be compared to the age calculated based on the GIID date of birth;

"**Associate(s)**" means those colleagues or associates of Demo Users who have given their explicit consent for their personal data to be processed using the Demo Solution, in accordance with the Privacy Notice;

"**Attack**" means a combination of repetitions and conflicts identified by the sub-contractor that may indicate a synthetic identity attack;

"**Au10tix**" means Au10tix Ltd, an Israeli private company whose company number is 514553007), with address at 5B Hanagar St., Hod Hasharon, Israel, TransUnion's sub-contractor for the purpose of this Service Schedule;

"**Biometric Representation**" means a representation created through proprietary and/or licensed algorithms of the unique set of coordinates comprising a Facial Image captured through the Demo Solution;

"**Biometric Comparison**" means the Product Component which compares the Biometric Representation derived from the Document Face with the Biometric Representation derived from the Selfie Face;

"**Client Branding**" means logos, trade names or other trade marks that are owned by or licensed to the Client and/or members of its group that the parties have agreed are to be incorporated into the Demo Solution;

"**Client Console**" means the browser-based interface which allows the Client to view the Output;

"**Console User**" means those members of the Client's staff who are authorised (have been given unique user credentials) to access the Client Console;

"**Demo User**" means a member of the Client's staff who has been given an Access Link to carry out a Test Transaction and has given their explicit consent for their personal data to be processed using the Demo Solution, in accordance with the Privacy Notice;

"**Device Environment Attributes**" means information that may be captured or accessed by the sub-contractor using cookies or similar technologies placed on a Demo User's device in order to facilitate the operation of the Demo Solution, including Geolocation Data unless the GPS feature in a Demo User's mobile device has been switched off or the device does not have access to GPS;

"**Document Face**" means the Facial Image contained in a GIID, either on the face of the GIID or within the NFC Chip (where available);

"**Documentation**" means the sub-contractor's instructions, guides (including technical guides) and manuals made available to the Client by TransUnion, any drawings, diagrams, designs, pictures or other images, tapes, disks or other devices or records embodying information in any form as published by TransUnion and/or the sub-contractor and/or made generally available by TransUnion and/or the sub-contractor in relation to the use of the Services and/or sales and marketing materials;

"**Facial Image**" means an image of a natural person that may be used for the purposes of allowing or confirming the unique identification of that person;

"**Geolocation Data**" means the geographical location information (in longitude and latitude format) that is collected from a Demo User's device using where enabled and consented to by the Demo User;

"**GIID**" means a Government-issued ID document, which includes a Facial Image;

"**GIID Verification**" means the Product Component which analyses a GIID in order to ascertain its authenticity and validity;

"**Good Industry Practice**" means the exercise of that degree of skill, diligence, prudence and foresight which would ordinarily be expected from a skilled and experienced operator engaged in providing services of the same kind as the Services seeking to comply with its contractual obligations and all Laws relating to the Services;

"**GPS**" means Global Positioning System and is a device feature that uses satellite data to calculate the geographical position of the device;

"**Infringement Claim**" includes any claim by a third party that use of the Services (including any software) or Documentation infringes, allegedly infringes, violates or constitutes a wrongful use of any third party's IPR or other proprietary rights of any person;

"**IPR**" means all forms of intellectual property rights and protections throughout the world, including, but not limited to, any (a) patents (including any patent applications, together with all reissuances, continuations, continuations-in-part, revisions, extensions and re-examinations thereof); (b) copyrights; (c) internet domain names, trade marks, service marks, and trade dress, together with all goodwill associated therewith; (d) trade

TransUnion

secrets; (e) rights in databases and designs (ornamental or otherwise); (f) moral rights, rights of privacy, rights of publicity and similar rights; and (g) any other proprietary rights and protections, whether currently existing or hereafter developed or acquired, whether published or unpublished, arising under statutory law, common law, or by contract, and whether or not perfected, including all applications, disclosures and registrations with respect thereto;

"**Malicious Code**" means any "virus" or "worm", "Trojan horse", "trapdoor", "software switch", "time bomb" or "logic bomb", "disabling code" or "disabling routines", "expiration dates", "protect codes", "data destruct keys", "worms", and other harmful or malicious code, files, scripts, agents, or programs;

"**NFC Chip**" means the Near Field Communication chip embedded in some GIIDs containing the personal information printed on the GIID in addition to an electronically encoded copy of the photograph of the GIID holder that was supplied at the point of issue of the GIID, which can be used to assist in the authentication of the identity of the GIID holder;

"**OCR Data Extraction**" means the extraction of data via the application of proprietary optical character recognition technology;

"**PECR**" means the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended from time to time;

"**Privacy Notice**" means the information notice displayed on the Demo Solution prior to commencement of each Test Transaction (a copy of which can be provided on request);

"**Proof of Liveness**" means the Product Component which assists in determining whether the Facial Image captured by the Demo Solution is from a live individual or is an image or video displayed on a video screen and can, if enabled, provide an Age Estimation;

"**Selfie Face**" means the Facial Image that appears in a photograph taken by the Demo User of themself and used as part of the processing for Proof of Liveness and/or Biometric Comparison Product Component(s);

"**Serial Fraud Monitor**" means the Additional Option which assists the Client in identifying potential fraud and/or an Attack by comparing the Input from the current Test Transaction with Output stored in the 'closed garden' database held by the sub-contractor which contains Output contributed by the Client only;

"**Test Transaction**" means the submission of Input via the Demo Solution for processing via the Product Components (including, where applicable, Additional Options) to produce the Output; and

"**TransUnion Client Service Desk**" which may be contacted via email at: clientservicedesk@transunion.co.uk or by telephone on 0845 120 1222.

4.2 **Operation of the Demo Solution**

4.2.1 The Client is permitted to have a maximum of ten (10) Console Users.

4.2.2 The Client is permitted to undertake up to 100 Test Transactions in total (not per Console User).

4.2.3 The Demo Solution shall be made available to Demo Users to commence a Test Transaction via an Access Link. A unique Access Link will be required for each Test Transaction.

4.2.4 TransUnion warrants that the Services shall be free from material defects. However, the following are excluded from such warranty:

4.2.4.1 defects discovered in any component of the Service that has been modified, altered, or enhanced without TransUnion's prior written consent;

4.2.4.2 defects resulting from or occurring from any act taken or omission not taken by TransUnion or the sub-contractor;

4.2.4.3 defects due to the Client's system; or

4.2.4.4 any defects arising from the use of the Services otherwise than in accordance with the terms and conditions of this Agreement & Service Schedule.

4.2.5 TransUnion is the first line of support, and the Client agrees that it will request assistance from TransUnion via its TransUnion Client Service Desk in respect of any support issues that arise in relation to the Services. The Client further agrees that it will not contact the sub-contractor directly except with the prior agreement of TransUnion.

4.2.6 The Client shall ensure that each Console User keeps their user credentials for access to the Client Console confidential and does not share them with other individuals. Where abuse is suspected, TransUnion reserves the right to suspend the account in question pending an investigation.

4.2.7 The Client agrees that it shall only use the Demo Solution in respect of Demo Users who are resident in the UK, Isle of Man or the Channel Islands.

4.3 **Data Protection**

4.3.1 The Client acknowledges that TransUnion acts as a controller in respect of the Console Users' and Demo Users' personal data and that it shall process such personal data in accordance with the Privacy Notice. The Client acknowledges that the Privacy Notice informs Console Users and Demo Users of how their personal data will be processed for the purposes of the Demo Solution only.

4.3.2 The Client acknowledges that some of the Services involve the processing of biometric data for the purpose of uniquely identifying a natural person, which is a special category of personal data under the GDPR, and that collection of Device Environment Attributes involves the placing of cookies or similar technologies on the End User's device.

4.3.3 The Client shall take responsibility for ensuring that its Demo Users make clear to any Associates whose personal data is captured and uploaded to the Demo Solution the details of how and why their personal data will be processed (in accordance with the Privacy Notice) and that the Associates have given their explicit consent for it to be used in this manner.

4.4 **Intellectual Property**

4.4.1 Without prejudice to clause 6.2 of the General Terms, any intellectual property rights in the Client Branding shall at all times remain vested in the Client (or its third party licensors) and neither TransUnion nor the sub-contractor shall acquire any rights in them save as expressly provided in this Service Schedule.

4.4.2 The Client grants to TransUnion and the sub-contractor a non-exclusive, royalty-free licence for the term of this Service Schedule to use the Client Branding solely for inclusion in the Demo Solution, where relevant, and/or to the extent necessary for TransUnion to provide the Services described in this Service Schedule.

4.4.3 TransUnion grants to the Client a non-transferable, revocable, non-exclusive, non-sublicensable licence to use and copy the IPR of TransUnion or its third-party licensors contained in the Services strictly only for the purpose of exercising the Client's rights and performing its obligations under this Service Schedule. All rights not expressly granted to the Client are reserved by the sub-contractor and its licensors. The Au10tix name, the Au10tix logo and the certain product names associated with the Service are trade marks of the sub-contractor the Company, TransUnion or third parties, and no right or license is granted to use them. The sub-contractor's trade marks are set out via a link on the sub-contractor's website that TransUnion shall make available to the Client on request.

4.4.4 The Client shall not knowingly:

4.4.4.1 use the Services to store or transmit infringing, libellous or otherwise unlawful or tortious material, or to store or transmit in violation of third-party rights;

4.4.4.2 interfere with or disrupt the integrity or performance of the Services; or

4.4.4.3 attempt to gain unauthorised access to the Services or the sub-contractor's related systems or networks.

4.4.5 The Client shall not:

4.4.5.1 alter, modify, translate, reproduce or create derivative works of the Services, or any part thereof;

4.4.5.2 attempt to derive the source code of the Services, reverse engineer, decompile or disassemble the Services or otherwise reduce the software embodied therein to human-perceivable form, or encourage or assist third parties in doing so.

4.4.6 For the avoidance of doubt, neither TransUnion (nor the sub-contractor) shall be liable for any Infringement Claim to the extent that such liability is based upon or arising from (a) use of the Services in a manner not in accordance with the Documentation, (b) modifications to the Services by anyone other than TransUnion or the sub-contractor; (c) connection or combination of a Service with any third party software or hardware not approved in writing by TransUnion or the sub-contractor where such connection or combination is the sole cause of an infringement, or where such liability is directly the result of the Client's (or any Demo User's) continued use of an infringing version of the Services when the current version of the Services has been modified to be non-infringing and TransUnion has provided the Client with such non-infringing version in accordance with clause 3.2 of the General Terms.

4.4.7 The Client warrants that it will apply standards and controls in accordance with Good Industry Practice to try to prevent transmission to TransUnion or the sub-contractor of any Malicious Code.

4.5 **Disclaimer of warranties**

4.5.1 The Service and all content are provided to the Client strictly on an "as is" and "as available" basis. To the maximum extent applicable by law, TransUnion, the sub-contractor, and its licensors make no other representation, warranty (whether statutory, express, implied or otherwise) or guarantee as to the availability, timeliness, truth, accuracy, reliability, suitability, merchantability, completeness or non-infringement of the Service or any content except as expressly stated in this Service Schedule. Without derogating from the generality of the foregoing and except as expressly stated in this Agreement, TransUnion does not represent or warrant that: (a) the use of the Service will be timely, uninterrupted, error-free or operate in combination with any other hardware, software, system or data; (b) the Service will be of satisfactory quality, performance or accuracy; or (c) the Service will meet the Client's requirements or expectations.

4.5.2 The Service may be subject to limitations, delays and other problems inherent in the use of the internet and electronic communications. TransUnion accepts no responsibility for any delays, delivery failures, or other damage resulting from such problems to the extent caused by the Client's equipment, systems or internet or electronics communications provider(s).

4.5.3 For the avoidance of doubt, and to the maximum extent permitted by law, except for any warranties expressly stated in this Agreement, the entire risk arising out of the Client's use of the Services remains with the Client.

SERVICE SCHEDULE
DOCUMENT VERIFICATION FACIAL BIOMETRICS (IDMISSION) ONLINE

Commented [MS5]: This Service Schedule contains all options - the Schedule will need to be tailored to reflect the particular options and permitted purposes applicable for the relevant client at Call-Off stage. Therefore, not all provisions in this Service Schedule will be applicable at the Call-Off stage.

1. **DESCRIPTION OF THE SERVICES**

In this Service Schedule, the Services shall comprise the following:

- **Solution(s)**: Mobile SDK, Web SDK, Identity Verification as a Service (or "IDaaS"), Submission API;
- **Product Component(s)**: GIID Verification, Proof of Liveness and Biometric Comparison, Additional Document Processing;
- **Additional Options**: Biometric Authentication, Manual Review, QR Code/URL provision, UK only hosting;
- **Results Interface(s)**: Client Portal access, Post Processing Webhook, Data Retrieval API;
- DVFB PoC;
- Data Storage;
- Access to Sandbox Facility;
- Pre-Sales Consultancy; and
- Maintenance and support services.

2. **PERMITTED PURPOSE**

2.1 To assist the Client with identity verification and/or anti-money laundering and/or the detection/prevention of fraud or financial crime, for the Client's internal business purposes only.

2.2 For the DVFB PoC only, to assist the Client in its assessment of the Services for the purposes of identity verification and/or anti-money laundering and/or the detection/prevention of fraud or financial crime. The Client agrees that the Output and the results of the Client's internal evaluation shall not be used by the Client in a live production environment or to build a scorecard(s). For the avoidance of doubt, unless this Service Schedule is terminated in accordance with paragraph 3.2, the permitted purpose in paragraph 2.1 shall apply on and from the day immediately following the end of the DVFB PoC.

3. **SERVICE SCHEDULE DURATION**

3.1 Insert Details (Where Applicable)As set out in the Primary ScheduleSubject to paragraph 3.2, Insert Details (Where Applicable)as set out in the Primary Schedule

3.2 The Client is permitted to terminate this Service Schedule at any time in the first thirty (30) days after the Service Start Date by giving TransUnion not less than seven (7) days' written notice (i.e. the last day to serve such notice shall be twenty three (23) days after the Service Start Date ("**DVFB PoC Termination**"). Any purported notice of DVFB PoC Termination served after the twenty third day following the Service Start Date shall have no effect.]

4. **SERVICE CONDITIONS**

These Service Conditions shall apply in respect of the Services.

4.1 In respect of these Service Conditions the following additional definitions apply:

"**Additional Document**" means an identity document that is not a GIID and which has been photographed by the End User;
"**Additional Document Processing**" means the processing of Additional Document using OCR Data Extraction;
"**Biometric Authentication**" means the service which includes a Proof of Liveness check and which compares a Biometric Representation of the End User's Selfie Face with a Biometric Representation of that End User's previously Enrolled Selfie Face, in order for the End User to authenticate their identity;
"**Biometric Comparison**" means the Product Component which compares the Biometric Representation derived from the Document Face with the Biometric Representation derived from the Selfie Face;
"**Biometric Representation**" means a representation created through proprietary algorithms of the unique set of coordinates comprising a Facial Image captured through the Solutions;
"**Client Branding**" means one or more of the fonts, logos, colours, trade names or other trade marks that are owned by or licensed to the Client and/or members of its group that the parties have agreed are to be incorporated into the Solution;
"**Client Portal**" means the portal which allows the Client to access the Data Storage on a read-only basis and to view the Processing Output;
"**Client Portal Users**" means those Client Users who are authorised (have been given unique user credentials) to access the Client Portal and have been appropriately trained in accordance with paragraph 4.8.7;
"**Client User Data**" shall mean any data relating to a Client User that is provided to TransUnion or the Sub-processor to enable the Client User to access the Services (including the Client Portal and the TransUnion Client Service Desk);
"**Client Users**" shall mean those members of the Client's staff who are users of the Services;
"**Data Retrieval API**" means the Results Interface that allows direct delivery of the Processing Output to the Client via an API;
"**Data Storage**" means the backend database, hosted by the Sub-processor, which contains (subject to the Client's requirements in relation to data retention referred to in paragraph H of Annex 1) all of the Processing Output and which may, dependent on the Solution taken and the Client requirements, be accessed via the Results Interfaces;
"**Device Metadata**" means information that may be captured or accessed (with the consent of the End User) using cookies or similar technologies from an End User's device and which may include IP address, device make and model, operating system (and version) of the device and Geolocation Data. It is used to optimise the effectiveness of the proprietary software;
"**Document Face**" means the Facial Image contained in a GIID, either on the face of the GIID or within the NFC Chip (where available);
"**Documentation**" means the guides (including the Integration Guide and the Portal Guide), manuals, drawings, diagrams, designs, pictures or other images, tapes, disks or other devices or records embodying information in any form as published by TransUnion and/or the Sub-processor and/or made generally available by TransUnion and/or the Sub-processor in relation to the use of the Services and/or sales and marketing materials;
"**DVFB PoC**" means the programme lasting 30 days and commencing on and from the Sign Up Date, which allows the Client to trial the Services (including the Solutions, Product Components, Additional Options (but not Manual Review) and Results Interfaces specified in paragraph 1) using the Sandbox Facility subject to the permitted purpose set out in paragraph 2.2 and the restrictions set out in paragraph 4.4.2;
"**End User**" means a customer or potential customer of the Client's products/services and, for the purposes of a DVFB PoC, may also be a member of the Client's staff who is a user of the Solution;
"**Enrolment**" means the storing of a Biometric Representation along with the Selfie Face and (as required by the Client), Document Face, an image of the GIID and/or other identifiers within the Data Storage for future re-use as part of Biometric Authentication ("Enrol" and "Enrolled" should be similarly interpreted);
"**Facial Image**" means an image of a natural person that may be used for the purposes of allowing or confirming the unique identification of that person;
"**Geolocation Data**" means the geographical location information (in longitude and latitude format) that is collected from an End User's device

using GPS;
"**GIID**" means a Government-issued ID document, which includes a Facial Image;
"**GIID Verification**" means the Product Component which analyses a GIID in order to ascertain its authenticity and validity;
"**Good Industry Practice**" means the exercise of that degree of skill, diligence, prudence and foresight which would ordinarily be expected from a skilled and experienced operator engaged in providing services of the same kind as the Services seeking to comply with its contractual obligations and all Laws relating to the Services;
"**GPS**" means Global Positioning System and is a device feature that uses satellite data to calculate the geographical position of the device;
"**Identity Verification as a Service"** or **IDaaS**" means the browser-based service that is hosted by the Sub-processor which enables the Product Components to be presented to End Users, and is available via commercially available web and mobile optimised browsers;
"**IDmission**" means IDmission LLC, 1830 17th St, Suite 100, Boulder, CO 80302;
"**Infringement Claim**" includes any claim by a third party that use of the Services, Solutions, SDK Software or Documentation infringes, allegedly infringes, violates or constitutes a wrongful use of any third party's IPR or other proprietary rights of any person;
"**Integration Guide**" means the guide(s) which shall be made available to the Client by TransUnion or the Sub-processor and which provide information regarding APIs and SDK as well as details of the GIID types supported, ISO country codes, ISO state codes, status codes and status code descriptions;
"**Intellectual Property Rights**" means all copyrights, moral rights, patents, trade marks, trade names, service marks, design rights (registered and unregistered), database rights, rights in goodwill, rights in know-how, trade secrets and inventions (whether patentable or not) and all other intellectual property rights (whether registered or not) and applications for and the right to apply for such rights anywhere in the world that may exist or come into existence from time to time;
"**Malicious Code**" means any "virus" or "worm", "Trojan Horse", "trapdoor", "Software Switch", "time bomb" or "logic bomb", "disabling code" or "disabling routines", "expiration dates", "protect codes", "data destruct keys", "worms", "time bombs", and other harmful or malicious code, files, scripts, agents, or programs;
"**Manual Review**" means the manual review of information submitted by the relevant Solutions where the Product Components selected have not been able to provide a conclusive result;
"**Mobile SDK**" means the software development kit that is used to assist the Client in building mobile applications for iOS and Android platforms. It enables the Product Components to be presented to End Users, via incorporation into the Client's own mobile app;
"**NFC Chip**" means the Near Field Communication chip embedded in some GIIDs containing the personal information printed on the GIID in addition to an electronically encoded copy of the photograph of the GIID holder that was supplied at the point of issue of the GIID, which can be used to assist in the authentication of the identity of the GIID holder;
"**OCR Data Extraction**" means the extraction of data via the application of proprietary optical character recognition technology;
"**PECR**" means the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended from time to time;
"**Post Processing Webhook**" means the facility for the Client to electronically receive the Processing Output direct from the Data Storage;
"**Pre-Sales Consultancy**" means the consultancy work undertaken by TransUnion and/or the Sub-processor in exploring the Client's requirements and Solution options;
"**Processing Input**" as defined in the Data Processing Annex;
"**Processing Output**" as defined in the Data Processing Annex;
"**Proof of Liveness**" means the Product Component which assists in determining whether the Facial Image captured by the Solution is from a live individual or is an image or video displayed on a video screen;
"**QR Code/URL Provision**" means the making available of a QR code/URL that directs the End User to the start of an ID verification journey via the Solutions; the QR code/URL may be static/generic or dynamic/personalised to the End User;
"**Sandbox Facility**" means the environment hosted by the Sub-processor which allows TransUnion's clients to test out Solutions, Product Components and Results Interfaces and/or run a DVFB PoC;
"**SDK Software**" means the software applications provided and licensed by TransUnion to the Client as further detailed in this Service Schedule;
"**Selfie Face**" means the Facial Image that appears in a photograph taken by the End User of themself and used as part of the Transactional Processing for Biometric Authentication and/or Proof of Liveness and/or Biometric Comparison Product Component(s);
"**Service Start Date**" means, for the purposes of this Service Schedule, the Sign Up Date;
"**Sign Up Date**" means from the date on which the Client receives the credentials to access the Sandbox Facility;
"**Submission API**" means an application programming interface which enables a Client to submit Processing Input to the Sub-processor for Transactional Processing;
"**Transaction**" means a completed End User journey where the End User has completed the Transactional Processing without error and the results have been delivered via the Results Interface. For the avoidance of doubt, a Transaction is completed regardless of a pass/fail result;
"**Transactional Processing**" means the capture of the Processing Input by the Solution and subsequent processing by the Product Components and where applicable the Additional Options, as further detailed in paragraph C(ii) of Annex 1;
"**TransUnion Client Service Desk**" which may be contacted via email at: clientservicedesk@transunion.co.uk or by telephone on: 0845 120 1222;
"**Web SDK**" means the software development kit used to build the web browser applications, which enables the Product Components to be presented to End Users, via the Client's own website.

4.2 The Sub-processor

4.2.1 TransUnion has appointed IDmission as its sub-processor in relation to the Services and, for the purposes of Article 28(2) of the GDPR, hereby gives its specific written authorisation to TransUnion to use IDmission as its processor (the "**Sub-processor**").

4.2.2 As a result of TransUnion's reliance on the Sub-processor for the delivery of the Services, clause 14.1 of the General Terms shall be extended to cover an Event of Force Majeure suffered by the Sub-processor. In such circumstances, TransUnion shall procure that the Sub-processor shall comply with the provisions of clause 14.2 and in the event that TransUnion is unable to perform its obligations under this Service Schedule by reason of the Sub-processor's Event of Force Majeure for a period of more than four weeks, TransUnion may terminate this Service Schedule immediately by serving notice on the Client and shall not be liable to the Client by reason of such termination.

4.3 Implementation Plan

4.3.1 A meeting (or meetings) shall be held between the parties prior to Services Commencement, during which an implementation plan and schedule of works (the "**Implementation Plan**") will be discussed and agreed.

4.3.2 To the extent that the Client wishes to make any amendments after the parties have agreed the Implementation Plan, TransUnion reserves the right to charge an additional fee in respect of professional service hours that will be incurred. Where TransUnion intends to invoke this right, it shall give notice to the Client of the estimated professional service hours and related fee before implementing the requested changes.

4.3.3 The Client shall at all times co-operate with TransUnion and provide TransUnion and/or the Sub-processor with such information and assistance as TransUnion may reasonably require in order to enable TransUnion and the Sub-processor duly and punctually to perform to meet the Implementation Plan.

4.4 Sandbox Testing

4.4.1 In order to test out the Solutions, Product Components (excluding Manual Review) and Results Interfaces and/or to run a DVFB PoC, the Sub-processor shall make available to the Client the Sandbox Facility.

4.4.2 The Client is permitted to perform Transactional Processing through the Sandbox Facility on End Users a maximum of 100 times per day for a maximum period of 30 days commencing on the Sign Up Date. Thereafter, the Client may with the agreement of TransUnion make further use of the Sandbox Facility as required for testing purposes with the same daily limit.

4.4.3 For the avoidance of doubt, where the Client uses the Sandbox Facility for the purposes of a DVFB PoC, and the Client wishes to add to or amend any of the Solutions, Product Components, Additional Options and/or Results Interfaces specified in paragraph 1, then the Client shall terminate this Service Schedule in accordance with paragraph 3.2 or enter into a letter of variation to amend this Service Schedule to properly reflect the Services to be taken on an ongoing basis.

4.4.4 The Client agrees to comply with TransUnion's rules and guidance on accessing the Sandbox Facility (as varied from time to time) (a copy of which is available to the Client upon request).

4.5 QR Code/URL Provision

4.5.1 Where the dynamic QR Code/URL Provision is taken, TransUnion may at the Client's initiation procure that the Sub-processor (or its sub-processor) shall send a QR code via email or SMS text message direct to End Users whose contact details have been provided by the Client. The Client warrants that such End Users have, in accordance with Applicable Law, given their permission to receive a communication in this manner.

4.5.2 Where a static/generic QR Code/URL is provided to the Client to provide to an End User, the End User will be required to enter a unique identifier (i.e. email address or mobile number) into the interface implemented by the Solution.

4.6 Device Metadata Capture

4.6.1 Where Device Metadata capture is switched off, the performance of the SDK Software and the Processing Output may be compromised.

4.6.2 Device Metadata capture involves the placing of cookies or similar technologies on the End User's device. The Client warrants to TransUnion that, in compliance with the Applicable Law (including PECR), all appropriate notices have been given and applicable consents have been obtained to enable the setting and reading of such cookies.

4.6.3 Unless the GPS feature in an End User's mobile device has been switched off or the device does not have access to GPS, Geolocation Data will be captured as part of the Device Metadata.

4.7 Solutions and Product Components

4.7.1 Some of the Services involve the processing of biometric data for the purpose of uniquely identifying a natural person, which is a special category of personal data under the GDPR.

4.7.2 The Client warrants to TransUnion that, in compliance with the Applicable Law (including Data Protection Legislation), consent has been obtained by the Client, and appropriate notices have been given to End Users, to enable the data provided by the End Users to be processed in the manner described in this Service Schedule, including paragraph 4.7.1, and the Data Processing Annex.

4.7.3 For the avoidance of doubt, Clients must obtain the consent of the End User and ensure the End User is provided with the appropriate notice before End Users commence the ID Verification journey directing End Users to the IDaaS landing page.

4.7.4 The IDaaS implements a generic ID verification journey and Client Branding options are limited to logo.

4.7.5 The End User will be required to agree to the Sub-processor's terms of use for IDaaS. The Client further acknowledges that the Sub-processor has a right to suspend access (temporarily or permanently) to IDaaS or features of the service (or to create usage limits) in respect of a particular End User where such End User in the opinion of the Sub-processor violates any provision of its terms of use of the service. A copy of the terms is available on request from TransUnion.

4.7.6 The Client shall not oblige End Users to use the Solutions for the purposes of identity verification and shall offer alternative methods by which an End User can verify their identity and/or have their documents validated and shall not discriminate against an End User because of their refusal to agree to use electronic identity or document verification systems.

4.7.7 The Client acknowledges that the guides provided as part of the Documentation are only intended to represent guidance for the Client and any meaning attributed to a status code description, any messaging delivered to the End User and any action taken by the Client as a result of a status code provided is for the Client alone to determine.

4.8 Operation of the Results Interfaces

4.8.1 The Client shall provide a secure web listener URL in order to receive the Processing Output via the Post Processing Webhook.

4.8.2 The Client shall ensure that the Post Processing Webhook and request to the Data Retrieval API includes the same unique identifier that was included in the Processing Input in order to match to the specified transaction.

4.8.3 The personal data contained in the Processing Output received via the Post Processing Webhook and Data Retrieval API does not represent all of the personal data held by the Sub-processor on behalf of the Client and that, in order to comply with a data subject access request under the GDPR, the Client will need to make a Processor Request under paragraph 4.11.6.

4.8.4 The Client shall provide details of all Client Portal Users to TransUnion so that TransUnion can set up accounts for and issue user credentials to those Client Portal Users to enable them to access the Client Portal. For operational reasons, TransUnion may change Client Portal Users' credentials at any time.

4.8.5 The Client shall ensure that each Client Portal User keeps their user credentials for access to the Client Portal confidential. User credentials shall not be shared between individuals and, where abuse is suspected, TransUnion reserves the right to suspend the account pending an investigation.

4.8.6 The Client shall remain responsible for the actions of Client Portal Users who have been issued with user credentials until such time as TransUnion confirms receipt of the Client's request for a Client Portal User to be disabled.

4.8.7 The Client shall ensure that all Client Portal Users have undertaken appropriate training and have been provided with a copy of the Client Portal User Guide before they are permitted to access to the Client Portal.

4.8.8 The personal data displayed to Client Portal Users does not represent all of the personal data held by the Sub-processor on behalf of the Client and that, in order to comply with a data subject access request under the GDPR, the Client will need to make a Processor Request under paragraph 4.11.6.

4.9 Intellectual Property

4.9.1 Without prejudice to clause 6.2 of the General Terms, any intellectual property rights in the Client Branding shall at all times remain vested in the Client (or its third party licensors) and neither TransUnion nor the Sub-processor shall acquire any rights in them save as expressly provided in this Service Schedule.

4.9.2 The Client grants to TransUnion and the Sub-processor a non-exclusive, royalty-free licence for the term of this Service Schedule to use the Client Branding solely for inclusion in the Solutions (where relevant) and/or to the extent necessary for TransUnion to provide the Services described in this Service Schedule.

4.9.3 The Client shall indemnify TransUnion from and against any and all liabilities, damages, losses, claims, costs and expenses, including reasonable legal fees, which may be suffered or incurred by TransUnion (either directly or under an indemnity from TransUnion to the Sub-processor) as a result of any claim by a third party that any materials provided by the Client to TransUnion (or the Sub-processor) under this Service Schedule, when used by TransUnion (or the Sub-processor) in accordance with this Service Schedule, infringe the Intellectual Property Rights of the relevant third party, provided that such infringement does not arise as a result of, or in connection with any act or omission (other than use in accordance with the terms of this Agreement) of TransUnion (or the Sub-processor).

4.9.4 Each party acknowledges that Intellectual Property Rights subsisting in the other party's products or services, including in the case of TransUnion the Solution(s), the Product Component(s), the SDK Software, the Results Interfaces and the Documentation, are the property of that party or are provided under licence to that party. Neither party grants to the other any rights in its Intellectual Property Rights or data save as expressly provided for in this Service Schedule. Each party acknowledges to the other that damages may not be an adequate remedy for any actual or potential infringement of its Intellectual Property Rights and/or any breach by the other party of this paragraph 4.9.4 and accordingly agrees that, in addition to any other right or remedy open to it, each party may be entitled to immediate injunctive relief to restrain any actual or anticipated infringement or breach thereof.

4.9.5 TransUnion grants to the Client a non-transferable, revocable, non-exclusive licence to use and copy the Intellectual Property Rights of TransUnion or its third-party licensors contained in the Services strictly only for the purpose of exercising the Client's rights and performing its obligations under this Service Schedule.

4.9.6 The Client shall not knowingly:

4.9.6.1 use the Services to store or transmit infringing, libellous or otherwise unlawful or tortious material, or to store or transmit in violation of third-party rights;

4.9.6.2 interfere with or disrupt the integrity or performance of the Services; or

4.9.6.3 attempt to gain unauthorised access to the Services or the Sub-processor's related systems or networks.

4.9.7 The Client shall not:

4.9.7.1 copy, modify, adapt, reverse engineer, de-compile or disassemble or otherwise attempt to discern the source code of the SDK Software or any software applications included in the Services (or cause or permit others to do so) except to the extent that is permitted by law;

4.9.7.2 create derivative works of the SDK Software, including copying, framing, or mirroring any part of the software, other than copying or framing on its own intranets or otherwise for its own business purposes;

4.9.7.3 access the SDK Software in order to: (i) build a competitive product or service, or (ii) copy any features, functions, or graphics of the software, other than when using the SDK Software for the Client's own internal business purposes; or

4.9.7.4 remove any title, trademark, copyright and/or restricted rights notices or labels from the SDK Software or Documentation.

4.9.8 For the avoidance of doubt, neither TransUnion (nor the Sub-processor) shall be liable for any Infringement Claim to the extent that such liability is solely and directly the result of (a) modifications to the Services or SDK Software by anyone other than TransUnion or the Sub-processor; or (b) the Client's or any End User's continued use of an infringing version of the Services or SDK Software when the current version of the Services or SDK Software has been modified to be non-infringing and TransUnion has provided the Client with such non-infringing version in accordance with clause 3.2 of the General Terms.

4.10 Other obligations and acknowledgements of the Client

4.10.1 Subject to paragraph 4.10.2, TransUnion acts solely as processor on behalf of the Client in respect of the processing of personal data contained within the Processing Input and the Processing Output. The Client is the controller in respect of such personal data.

4.10.2 TransUnion acts as a controller in respect of any personal data contained within the Client User Data held by or on behalf of TransUnion. TransUnion shall and shall procure that the Sub-processor shall process such personal data in accordance with the notice displayed on the TransUnion website, at such URL as is notified to the Client from time to time.

4.10.3 The Client agrees that, where TransUnion is acting as processor, then paragraph 4.11 of these Service Conditions shall apply.

4.10.4 Without prejudice to clause 10.3 of the General Terms, TransUnion makes no representations as to the suitability of the Services for the purposes of compliance with any legislation or regulation. The Client is responsible for satisfying itself that the Processing Output meets any such requirement.

4.10.5 TransUnion is the first line of support and the Client agrees that it will request assistance from TransUnion in respect of any maintenance and support issues that arise in relation to the Services. The Client further agrees that it will not contact the Sub-processor directly except with the prior agreement of TransUnion.

4.10.6 The Client warrants that it will apply standards and controls in accordance with Good Industry Practice to try to prevent transmission to TransUnion or the Sub-processor of any Malicious Code.

4.10.7 The Client agrees that it shall only use the DVFB Services in respect of customers who are resident in the UK, Isle of Man or the Channel Islands.

4.11 Data Processor obligations

4.11.1 This Service Condition 4.11 only applies in relation to any personal data in the Processing Input and Processing Output and, for the purposes of this Service Schedule only, shall take precedence over clause 8 of the General Terms in the event of any inconsistency.

4.11.2 The parties acknowledge and agree that their respective statuses as controller or processor for the purposes of this Service Schedule are as set out in paragraph 4.10.1 and 4.10.2.

4.11.3 To the extent that TransUnion is acting as a processor of personal data on behalf of the Client in respect of this Service Schedule, it shall:

4.11.3.1 implement appropriate technical and organisational measures in such a manner that its processing of the personal data will meet the requirements of the Data Protection Legislation and ensure the protection of the rights of the relevant data subjects;

4.11.3.2 not engage another processor of the personal data without prior specific or general written authorisation of the controller and, where it relies on a general authorisation, inform the controller of any intended changes concerning the addition or replacement of other processors;

4.11.3.3 where it engages another processor for carrying out processing activities on behalf of the Client, impose obligations on that other processor that are substantially equivalent to the terms set out in this paragraph 4.11.3;

4.11.3.4 process the personal data only on documented instructions from the Client or as otherwise required by Applicable Law;

4.11.3.5 not transfer the personal data to an international organisation or to a place outside both the United Kingdom and the European Economic Area the United Kingdom other than on the documented instructions of the Client;

4.11.3.6 where processing personal data otherwise than on the basis of documented instructions from the Client, first inform the Client of the requirement to process it on grounds of Applicable Law, unless prohibited from doing so by Applicable Law;

4.11.3.7 ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

4.11.3.8 taking into account the nature of the processing, assist the Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests under the Data Protection Legislation in relation to the data subjects' rights of access to personal data, rectification of personal data, erasure of personal data, restriction of personal data, data portability, objection to

TransUnion

processing of personal data, and in relation to automated individual decision-making. Any such assistance shall be requested by the Client as a Processor Request in accordance with clause 4.11.6;

4.11.3.9 notify the Client without undue delay after becoming aware of a personal data breach affecting the data being processed;

4.11.3.10 taking into account the nature of the processing and the information available to the processor, assist the Client in ensuring compliance with its obligations under the Data Protection Legislation in relation to security of processing, notification of personal data breaches to regulatory authorities and to data subjects, and carrying out and consulting with regulatory authorities in relation to data protection impact assessments. Any such assistance shall be requested by the Client as a Processor Request in accordance with clause 4.11.6;

4.11.3.11 at the choice of the Client, delete or return the personal data to the Client after the end of the provision of the Services, and delete existing copies unless required to store it by Applicable Law;

4.11.3.12 make available to the Client all information necessary to demonstrate compliance with the obligations under the Data Protection Legislation in relation to the appointment and use of processors;

4.11.3.13 allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client, in accordance with clause 13 (Audit) of the General Terms; and

4.11.3.14 immediately inform the Client if, in its opinion, an instruction given by the Client infringes the Data Protection Legislation or any other Applicable Law relating to data protection.

4.11.4 For the purposes of paragraph 4.11.3.2:

4.11.4.1 the Client hereby gives TransUnion a general authorisation to appoint any other processor to process the Input and the Output in accordance with this Agreement;

4.11.4.2 if the Client objects to the appointment of a processor, the parties shall enter into good faith negotiations, during which time TransUnion may suspend the supply of the Services, with a view to agreeing an alternative processor acceptable to the Client and a variation to the Fees reflecting any consequential increase in TransUnion's costs; and

4.11.4.3 if the parties fail to reach an agreement under 4.11.4.2 within a period of 14 days, TransUnion may by written notice immediately terminate this Service Schedule (including all licences granted under it).

4.11.5 For the purposes of paragraphs 4.11.3.4, and 4.11.3.5, the terms of this Agreement (including the contents of the Data Processing Annex) are deemed to be documented instructions of the Client.

4.11.6 Where the Client wishes to make a change to the Services (including the documented instructions) or request assistance under paragraph 4.11.3.8 or 4.11.3.10, the Client shall notify TransUnion in writing (a "**Processor Request**").

4.11.7 As soon as practicable after receipt of the Processor Request, TransUnion shall specify whether it is able to effect the change/provide the requested assistance and if so what additional charge (if any) shall be levied on the Client.

4.11.8 Any Processor Request (and the appropriate charge to be levied) shall be agreed in writing between the parties and signed by appropriately authorised representatives.

4.11.9 Nothing in this Agreement shall relieve TransUnion of its own direct responsibilities and liabilities as a processor under the Data Protection Legislation.

4.12 Data Retention Instructions

4.12.1 TransUnion shall procure that the Sub-processor shall delete the Processing Input and Processing Output at the end of [INSERT NUMBER] [INSERT UNIT] from the date/time the Processing Input was received.

4.12.2 TransUnion shall procure that the Sub-processor shall delete the Device Metadata at the end of [INSERT NUMBER] [INSERT UNIT] from the date/time such data was collected from the End User's device.

4.12.3 TransUnion shall procure that the Sub-processor shall delete the Enrolled Data at the end of [INSERT NUMBER] [INSERT UNIT] from the date/time it was first collected.

4.12.4 TransUnion shall procure that the Sub-processor shall delete the End User communications data at the end of [INSERT NUMBER] [INSERT UNIT] from the date/time such data was received by the Sub-processor.

ANNEX 1 – DATA PROCESSING
DOCUMENT VERIFICATION FACIAL BIOMETRICS (IDMISSION)

This Data Processing Annex records certain details concerning the processing to be performed by TransUnion acting as a processor of personal data (and by IDmission as its sub-processor) on behalf of the Client pursuant to this Service Schedule. TransUnion may give notice to the Client of changes to the Data Processing Annex from time to time but only to the extent necessary to comply with record keeping obligations under the Data Protection Legislation.

Identity of the processor(s) and controller

Processor: TransUnion International UK Limited (company number 03961870), registered office: One Park Lane, Leeds, West Yorkshire LS3 1EP

Approved sub-processors: IDmission LLC, 1830 17th St, Suite 100, Boulder, CO 80302.

IDmission may also use other sub-processors to fulfil the Services; a full list shall be provided to the Client upon request.

Controller: [INSERT DETAILS OF CLIENT LEGAL ENTITY]

A. Subject matter of the processing
Carrying out Transactional Processing. The Processing Output is then stored by the Sub-processor in the Data Storage for access by/onward transmission to the Client.

Where taken by the Client, the QR Code/URL Provision may involve the Sub-processor sending out to End Users an email or SMS text message containing a QR Code/URL which will direct the End User to the start of their ID verification journey.

B. Duration of the processing
As set out in paragraph 3 of this Service Schedule (Service Schedule Duration), subject to earlier deletion of the data in accordance with paragraph H below.

C. Nature and purpose of the processing
TransUnion will process End Users' personal data as necessary to perform the Services described in this Service Schedule.

(i) QR Code/URL provision
- use and storage of End User email addresses and/or mobile telephone numbers ("**End User Communications Data**")
  Purpose: to contact the End User in order to start the ID verification journey and/or for Biometric Authentication.

(ii) GIID Verification:
- OCR Data Extraction
- (where appropriate) reading of the eChip from the GIID
- (where appropriate) use of cookies or similar technologies to extract Device Metadata
- (where appropriate and switched on by the End User) collection of Geolocation Data
- proprietary assessment of the End User's GIID to identify potential anomalies

Proof of Liveness:
- proprietary assessment of liveness of the captured Selfie Face

Biometric Comparison:
- biometric comparison of the captured Selfie Face and Document Face

Additional Document Processing:
- capture of Additional Document and OCR Extraction

Biometric Authentication
- proprietary assessment of liveness of the captured Selfie Face, and
- comparison of a Biometric Representation of a Selfie Face with a Biometric Representation of that End User's previously Enrolled Selfie Face
  Purpose: to enable Processing Output to be created.

(iii) Enrolment (only applicable if Client is taking Biometric Authentication):
- storage and retention of a Biometric Representation along with the Selfie Face, Document Face and/or an image of the GIID (as required by the Client)
  Purpose: to enable Processing Output to be retained for future authentication of the End User.

(iv) Results Interfaces and Data Storage:
- sorting, saving and storage of the Processing Input and Processing Output
- Client access to the Processing Output via the Client Portal (where appropriate)
- retrieval of Processing Output by the Client using the Data Retrieval API (where appropriate)
- receipt of Processing Output via the Post Processing Webhook (where appropriate)
- deletion of data in accordance with Client instructions (see paragraph H below)
  Purpose: to enable access and for record-keeping purposes.

D. Types of personal data
(i) **Processing Input**
- GIID image
- Data extracted from the GIID including name, address, date of birth, gender, nationality, document type, ID number(s), date of issue, date of expiry, issuing authority, place of issue, Document Face and image of the signature
- Where relevant, this may also include data extracted from the NFC Chip

- Where the Mobile SDK Solution is taken, Device Metadata including: IP address, device make and model, operating system/version and, where consented by the End User, Geolocation Data
- Where the Web SDK Solution is taken, Device Metadata including: IP address and operating system/version, browser/version, and, where consented by the End User, Geolocation Data
- Where Proof of Liveness, Biometric Comparison and/or Biometric Authentication is undertaken, a Selfie Face
- Where Additional Document Processing is taken, an image of the Additional Document and data extracted from it, primarily name and address
- Where the QR code/URL Service is taken, this may include End User email address and/or mobile phone number or other unique identifier

(ii) **Processing Output**
- Date and time stamp of the processing of the data
- Unique transaction ID
- Copy of the GIID image
- Information extracted from the face of the GIID as described in (i) above
- Information extracted from the NFC Chip, where relevant
- Document Face
- Where Additional Document Processing is taken, information derived from OCR Data Extraction and an image of the Additional Document
- Processing results including verification results, scores, error codes and fraud codes where applicable

(iii) **Special Category Data**
Where Proof of Liveness and/or Biometric Comparison and/or Biometric Authentication are taken, biometric data will be processed in the form of a Biometric Representation of the Facial Images presented through the GIID and the Selfie Face.

(iv) **Identifiers**
The personal data processed will also include a:
- Client identifier for each End User; and a
- Sub-processor identifier for each End User.

E. Categories of data subject
End Users who wish to purchase or consume products/services provided by the Client.

F. Security of processing
As set out in clause 8.11 and as further detailed within TransUnion's information security policies from time to time.

G. Transfers of personal data outside the UK or EEA
Personal data will be processed in the Republic of Ireland (unless the Client has requested UK only hosting – in which case data will be hosted in the UK but, for the Client support purposes, limited Client User and/or End User personal data may be processed in the United States of America).

There will be no transfers of personal data outside the EEA unless the Client has selected the Manual Review (in which case, the personal data will be processed in India). Where the Client has requested UK only hosting, there will be no transfers of personal data outside the UK.

H. Ongoing data retention and deletion
- End User communications data (if appropriate)
  In accordance with the Client's documented instructions (as set out in paragraph 4.12 of this Service Schedule) ("**Data Retention Instructions**")
- Processing Input and Processing Output
  In accordance with the Data Retention Instructions
- Device Metadata
  In accordance with the Data Retention Instructions
- Enrolled Data (if appropriate)
  In accordance with the Data Retention Instructions
  In the absence of Data Retention Instructions, all data except Client User Data will be deleted after 72 hours.

I. Data retention or deletion upon completion of Services
On termination of this Service Schedule, TransUnion shall procure that the Sub-processor shall, unless prohibited from doing so by law, securely delete or destroy any remaining personal data contained relating to the Services in its possession or control.

J. Data Protection Officer details
Processor:
Rosie Horsewood, Legal Director
TransUnion Information Group, One Park Lane, Leeds, West Yorkshire, LS3 1EP
Email: dpo@transunion.co.uk
Sub-processor:
Name: Ankit Shah
Address: IDmission, TBC
Email: ankit.shah@idmission.com

SERVICE SCHEDULE
FRAUDFORCE (ONLINE)

Commented [MS6]: This Service Schedule contains all options - the Schedule will need to be tailored to reflect the particular options and permitted purposes applicable for the relevant client at Call-Off stage. Therefore, not all provisions in this Service Schedule will be applicable at the Call-Off stage.

1. **DESCRIPTION OF THE SERVICES**

In this Service Schedule, the Services shall comprise the following:

1.1 The provision of software (including, where appropriate, a software development kit) designed to collect certain device technical data and user interaction attributes (the "**Device Identifying Software**"), which must be installed on the Client's website and/or mobile app;

1.2 Integration support;

1.3 FraudForce, delivered via iovation's API including: (the "**FraudForce Service**");

- SureScore
- Advanced Transactional Model
- IP Reputation Lite

(the "**FraudForce Service**");

1.4 Access to the Intelligence Center;

1.5 Set up and maintenance of an ("API") in respect of the FraudForce Service.

1.6 API access to a data storage facility that allows the Client to download certain information on transactions they have processed through the FraudForce Service ("**Transaction Storage Service**").

2. **PERMITTED PURPOSE**

2.1 To identify suspicious and/or high risk devices used by individual users that access the Client's website and/or mobile app, for the Client's internal business purposes only.

3. **SERVICE SCHEDULE DURATION**

3.1 Insert Details (Where Applicable)As set out in the Primary Schedule.

4. **SERVICE CONDITIONS**

These Service Conditions shall apply in respect of the Service.

4.1 In respect of these Service Conditions, the following definitions apply:

"**Business Rules**" means the underlying business rules designed to assess the risk of fraud associated with a particular device and which are configurable to suit a particular sector and/or client risk profile;

"**FraudForce Output Data**" means the output data provided to the Client as a result of using the FraudForce Service;

"**FraudForce Input Data**" means the device technical data and user interaction attributes (including personal data) that is collected from individual users of the Client's website and/or mobile app;

"**Fraud Database**" means the database of known devices, which enables TransUnion to provide the FraudForce Service to its clients;

"**Fraud Updates**" means evidence regarding accounts and devices determined to be associated with fraud or abuse;

"**Intelligence Center**" means the facility which allows the Client to obtain individual reporting, view Transaction Insight Data, change Business Rules and contribute Fraud Updates;

"**iovation**" means iovation Inc, a Delaware corporation with a place of business at 555 W. Adams St, Chicago, Illinois 60661, for the purposes of this Service Schedule TransUnion's subcontractor;

"**Transaction Insight Data**" means the optional application and / or transaction data (including personal data such as email address and/or billing address) that are collected from or associated with individual users of the Client's website and/or mobile app.

4.2 The FraudForce Service and the FraudForce Output Data are licensed to the Client by TransUnion on a non-exclusive basis only.

4.3 The Client agrees to install the Device Identifying Software on its website and/or mobile app and utilise such Device Identifying Software on a non-exclusive basis.

4.4 The Client acknowledges that the provision of the FraudForce Service requires TransUnion and/or its subcontractor to transfer the FraudForce Input Data, the Transaction Insight Data (including personal data contained within such Input) to third parties located in countries or territories outside of both the United Kingdom and European Economic Area. The licence granted by the Client at clause 6.3 of the General Terms is granted in full contemplation of and agreement to such transfers. Any such transfers shall be performed in accordance with the Data Protection Legislation.

4.5 The Client warrants to TransUnion that, in compliance with the Applicable Law (including the Data Protection Legislation), applicable consent has been obtained, and appropriate notices have been given to its customers, that the data relating to those data subjects may be processed in the manner described in paragraphs 4.4, 4.14 and 4.16. This notice shall include a link to (i) the TransUnion Bureau Privacy Notice, currently available at https://www.transunion.co.uk/legal/privacy-centre/pc-bureau; and (ii) the iovation privacy policy currently available at https://www.iovation.com/privacy, (or in either case, such replacement URL as notified to the Client from time to time).

4.6 The Client acknowledges that iovation will provide all after sales support. The contact email for support and queries relating to the FraudForce Service (to be used instead of the email address shown in the Primary Schedule) is TruValCSupt@transunion.com.

4.7 Without prejudice to clause 5.7 of the General Terms, if the FraudForce Output Data contains a system error message, this is an indicator that either the system has timed out or that there is an internal system issue and no assumption should be made by the Client (on the basis of this error message) as to the fraud risk associated with the particular FraudForce Input Data that resulted in the system error message.

4.8 The Client shall not create or attempt to create (or permit others to create or attempt to create), by reverse engineering or otherwise, the source programs or any part thereof from the object programs or from any other information made available to it by TransUnion or its subcontractor under this Agreement and shall not decompile, disassemble, modify, alter or create derivative works of the Service. Liability for a breach of this Service Condition shall be unlimited, notwithstanding the liability provisions set out in clause 10 of the General Terms.

4.9 The Client agrees that it shall only use the FraudForce Service in respect of customers who are resident in the UK, Isle of Man, the Channel Islands, the EEA or the USA.

4.10 The Client acknowledges that the FraudForce Service is not intended to be indicative of a customer's creditworthiness or eligibility for insurance. Without prejudice to paragraph 2 of this Service Schedule (Permitted Purpose) and clause 5.1.1 of the General Terms, the Client warrants that it shall not use the Output from the FraudForce Service as a factor in establishing any customer's eligibility for credit or insurance.

4.11 The Client shall not use the FraudForce Service as the sole basis for any business decision. Without prejudice to clause 8.10 of the General Terms, the Client shall not use the FraudForce Service (including any Output) to make a decision based solely on automated processing (including profiling) in relation to a data subject where such decision produces legal effects concerning that data subject or similarly significantly affects that data subject (including entirely preventing a data subject from signing up or accessing the Client's services) except where the Client is permitted to do so pursuant to the Data Protection Legislation. Where it is so permitted to make such decision, the Client shall at all times comply with all relevant requirements as set out under the Data Protection Legislation in relation to that data subject's rights and freedoms and legitimate interests in connection with that decision.

4.12 Nothing contained in this Agreement shall be construed as granting or conferring any right, title, or interest, in any proprietary information, patent, trade mark, copyright, trade secret or other proprietary right in the FraudForce Service or Device Identifying Software that is now or subsequently owned by iovation or TransUnion.

4.13 The Client agrees that TransUnion and/or iovation will retain all ownership rights (including but not limited to any copyright, patent, trade secret, trade mark or other proprietary and/or intellectual property rights) in and to the Device Identifying Software, the FraudForce Service, the FraudForce Output Data and the Fraud Database (including but not limited to any components thereof, any information contributed to the Fraud Database as a result of the performance of this Agreement and any adaptation of the Device Identifying Software or the FraudForce Service to meet the Client's specifications, unless the adaptation incorporates intellectual property of the Client in which case such intellectual property will remain the Client's property) (together the "**FraudForce Elements**"). To the extent that any such rights may have vested in it, the Client hereby assigns to TransUnion all existing and future intellectual property rights in the FraudForce Elements and all materials embodying such rights to the fullest extent permitted by law.

4.14 The Client acknowledges that the FraudForce Service uses first party cookies (set by the Client) and third party cookies (set by TransUnion/iovation) for its data capture process.

4.15 The Client shall provide (or will procure that a third party acting on its behalf will provide) Fraud Updates on a regular basis by submitting such evidence via the Intelligence Center.

4.16 In respect of the FraudForce Service the Client grants to each of TransUnion and iovation a non-exclusive, irrevocable, perpetual licence to copy, store, use and sub-licence the Input (including the internet protocol addresses that form part of the Input) and the Fraud Updates to enable TransUnion and iovation to provide services to their clients in which the Input and the Fraud Updates are used to assist with identity verification and prevention of fraud/money laundering. This paragraph 4.16 shall survive the expiry or termination of this Agreement.

4.17 The Client acknowledges that neither TransUnion nor its subcontractor make any warranties or representations (i) as to the suitability of the FraudForce Service and FraudForce Output Data for any particular purpose; (ii) as to the accuracy or completeness of the FraudForce Output Data; or (iii) that the FraudForce Service will be uninterrupted or continuously available. For the avoidance of doubt, unless expressly stated to the contrary, all warranties provided by TransUnion as part of the General Terms are provided by TransUnion only.

4.18 Where requested by the Client, available Transaction Insight Data will be collected and will be accessible via the Intelligence Center.

SERVICE SCHEDULE
GEOFRAUD (BATCH)

Commented [MS7]: This Service Schedule contains all options - the Schedule will need to be tailored to reflect the particular options and permitted purposes applicable for the relevant client at Call-Off stage. Therefore, not all provisions in this Service Schedule will be applicable at the Call-Off stage.

1. **DESCRIPTION OF THE SERVICES**

In this Service Schedule, the Services shall comprise the following:

1.1 GeoFraud (Batch Service)

1.2 One-off batch processing ServiceOngoing batch processing ServiceOne off retrospective batch processing Service in respect of the periods: (1) [INSERT DATE PERIOD 1] and (2) [INSERT DATE PERIOD 2] ('**Retro Periods**')

1.3 **Input**

1.3.1 The Client shall provide TransUnion with one file comprising up to [INSERT VOLUME] customer records on a date to be agreed between the parties.

1.3.2 The Client shall provide TransUnion with a maximum of [INSERT VOLUME] customer records [INSERT FREQUENCY OF BATCH SUBMISSIONS]. Each file submitted by the Client shall comprise not less than [INSERT MINIMUM VOLUME PER FILE] customer records per file. The dates on which such files shall be provided to TransUnion shall be agreed between the parties from time to time.

1.3.3 The Client shall provide TransUnion with the Input files comprising up to the following customer records:

Input File Reference:	Volume of Customer Records:
Input File 1	[INSERT VOLUME]
Input File 2	[INSERT VOLUME]
Input File 3	[INSERT VOLUME]
Input File 4	[INSERT VOLUME]
Input File 5	[INSERT VOLUME]
Input File 6	[INSERT VOLUME]
Input File 7	[INSERT VOLUME]
Input File 8	[INSERT VOLUME]
Input File 9	[INSERT VOLUME]
Input File 10	[INSERT VOLUME]

Such files shall be provided to TransUnion on dates to be agreed between the parties.

1.3.4 The Client shall provide TransUnion with [INSERT OTHER DETAILS] customer records during each Year of this Agreement. The dates on which such files shall be provided to TransUnion shall be agreed between the parties from time to time.

1.3.5 [INSERT INPUT STATEMENT].

1.4 **Output**

1.4.1 The GeoFraud Service shall comprise batch processing by TransUnion of the Input [INSERT HOW MANY TIMES FILE IS BEING PROCESSED] against its databases, resulting in the Output comprising the Input appended with the relevant GeoFraud scores (where available).

1.4.2 The GeoFraud Service shall comprise a retrospective analysis by TransUnion of the Input [INSERT HOW MANY TIMES FILE IS BEING PROCESSED] against its databases, resulting in the Output comprising the Input appended with the relevant retrospective GeoFraud scores (where available).

2. **PERMITTED PURPOSE**

2.1 To assist the Client in prevention of fraud in respect of its internal business purposes only.

2.2 The Client is permitted to use the Output for its own internal evaluation purposes only.

3. **SERVICE SCHEDULE DURATION**

3.1 Insert Details (Where Applicable)As set out in the Primary ScheduleThis Service Schedule shall automatically terminate upon completion of the Services.

4. **SERVICE CONDITIONS**

These Service Conditions shall apply in respect of the Services.

4.1 The Client acknowledges that the Services may use SHARE data (as defined in, and subject to the terms of the paragraph entitled "**Closed User Group Data**" in the Primary Schedule).

PAYMENT SCHEDULE

The fees shall be as stated in the G-Cloud Call Off Contract.

GENERAL TERMS FOR TRANSUNION SERVICES

(VERSION T39-OM1 10/25)

1 DEFINITIONS AND INTERPRETATION

1.1 In this Agreement (unless the context requires otherwise) the following terms have the following meanings:

"**Agreement Effective Date**" means (unless otherwise stated in the Primary Schedule) the earlier of (i) the Agreement Signature Date; and (ii) the Service Start Date.

"**Agreement Signature Date**" means the date of signature of this Agreement or, if signed by the parties on different dates, the date of the last signature.

"**Applicable Law**" means any law, statute, statutory instrument, bylaw, order of a court of competent jurisdiction and any requirement of any regulatory, fiscal or governmental body to which the relevant party is subject, in all cases to the extent in force from time to time and which applies to the relevant party in undertaking any relevant activity pursuant to or in connection with the Agreement.

"**Authorised Data Processor**" means any third party expressly identified as an Authorised Data Processor in the Primary Schedule.

"**Authorised Group Company**" means in relation to the Client, any other company expressly identified as an Authorised Group Company in the Primary Schedule with which it is under Common Control. A company expressly identified as an Authorised Group Company in the Primary Schedule shall only be an Authorised Group Company for so long as it is a company under such Common Control.

"**Batch Services**" means such part of the Services described as "Batch Services" in a Service Schedule, including (where applicable) the Output of such Services.

"**Claims Management Company**" means any person: (i) carrying out one or more of the activities set out in sections 89G to 89M of the Financial Services and Markets Act 2000 (Claims Management Activity) Order 2018; and (ii) not falling within any of the exemptions at section 89N of that Order.

"**Client**" means the person or organisation named as the Client on the front page of this Agreement.

"**Client User Data**" shall mean all and any data relating to a Client User's access to the Services, including such data provided to TransUnion to enable the provision of the Services to the Client (for example, to enable TransUnion to create and allocate Client User log ins).

"**Client Users**" shall mean those members of staff of the Client, and those members of staff of any Authorised Data Processor or any Authorised Group Company who are authorised by the Client to access the Services.

"**Common Control**" means where one person Controls another or when two persons are Controlled by a third party, in all cases whether directly or indirectly.

"**Confidential Information**" means all trade secret and confidential or proprietary information of each party including (but not limited to) information concerning its products, services, customers, suppliers, business accounts, financial or contractual arrangements or other dealings, computer systems, test data, software, source and object code, business methods and development plans, contained in any format and whether or not communicated orally and whether or not marked "confidential". Without limiting the above, in the case of the Client's obligations, the term Confidential Information shall be deemed to include the Output and the Documentation, and in the case of TransUnion's obligations, the term Confidential Information shall be deemed to include the Input.

"**Consultancy**" means such part of the Services described as "Consultancy" in a Service Schedule, including (where applicable) the Output of such Services.

"Control" means in relation to a company, the power of a person to secure that the affairs of the company are conducted in accordance with the wishes of that person (a) by means of the holding of shares, or the possession of voting power, in or in relation to that or any other company; or (b) as a result of any powers conferred by the articles of association or any other document regulating that or any other company.

"**Data Management Services**" means such part of the Services described as "Data Management Services" in a Service Schedule, including (where applicable) the Output of such Services.

"**Data Protection Legislation**" has the meaning given in section 3(9) of the Data Protection Act 2018, together with any other applicable legislation relating to the processing of personal data; and "**personal data**", "**process**", "**processor**", "**controller**", "**personal data breach**" and "**data subject**" shall have the meanings given to such terms in the Data Protection Legislation.

"**Documentation**" means all user guides provided by TransUnion to the Client in respect of the Services.

"**EEA**" means the European Economic Area, as constituted from time to time.

"**ER Regulations**" means, as relevant: (i) the Representation of the People (England and Wales) Regulations 2001; (ii) the Representation of the People (Scotland) Regulations 2001; (iii) the Representation of the People (Northern Ireland) Regulations 2008; and (iv) the Registration of Electors Regulations 2003 (regulations enacted within the Isle of Man).

"**Event of Force Majeure**" means any cause beyond the reasonable control of the affected party, including any acts of God, flood, drought, earthquake or other natural disaster, epidemic, pandemic, collapse of buildings, fire, explosion, accident, terrorist attack, civil war, civil commotion or riot, war, threat of or preparation for war, armed conflict, imposition of sanctions, embargo, or breaking off of diplomatic relations, nuclear, chemical or biological contamination, sonic boom or electromagnetic pulse, industrial action, failure in telecommunications services or unauthorised interference with either party's systems or services via the internet, any law or any action taken by a government or public authority, including imposing an export or import restriction, quota or prohibition, or failing to grant a necessary licence or consent, in all cases including any consequences of, any governmental, regulatory, judicial or industry act undertaken, decision taken or guidance given in response to or otherwise in connection with, any such events or circumstances.

"**FCA**" means the Financial Conduct Authority or successor organisation fulfilling a materially similar regulatory function.

"**FSMA**" means the Financial Services and Markets Act 2000.

"**General Terms**" means these General Terms for TransUnion Services.

"**Input**" means all source data, materials and instructions made available to TransUnion pursuant to this Agreement (including, in respect of any Online Services, data input onto TransUnion's databases) by (or on behalf of) the Client to enable provision of the Services.

"**IPR**" means all copyright and related rights, database rights, trade marks, service marks, trade, business and domain names, rights in trade dress, get-up, goodwill or to sue for passing off, rights in designs, patents or confidential information (including know-how and trade secrets) and any other intellectual property rights, registered or unregistered, in any part of the world.

"**Minimum Security Standards**" means the minimum information security standards to be met by both parties as specified by TransUnion from time to time as the Minimum Security Standards on the web page https://www.transunion.co.uk/legal/client-minimum-security.

"**Notes**" means any additional terms and conditions relating to the charges which are identified as Notes in the Payment Schedule.

"**Online Services**" means such part of the Services described as "Online Services" in a Service Schedule, including (where applicable) the Output of such Services.

"**Output**" means any and all data, scores, results, reports, documents, specifications, flags, models, attributes, software, leads and other materials and information (and all updates of them) in any form to be made available to the Client by or on behalf of TransUnion, including the output from the Services and such output as is described in this Agreement, whether or not appended to the Input.

"**Permitted Purpose**" means, in respect of the Services, the relevant purpose described as such in the relevant Service Schedule.

"**Portfolio Services**" means such part of the Services described as "Portfolio Services" in a Service Schedule, including (where applicable) the Output of such Services.

"**Prohibited Material**" means anything pornographic, sexually explicit, offensive, racist, obscene, abusive, violent, criminal, defamatory, unlawful or illegal, and any other type of material specified as Prohibited Material in the relevant Service Conditions.

"**Prohibited Use**" means any use of the Output in connection with (i) tax evasion or aggressive tax avoidance schemes; (ii) private investigation services; (iii) direct marketing; (iv) any Prohibited Material; or (v) any other activity specified as a Prohibited Use in the relevant Service Conditions; in each case except to the extent expressly and specifically permitted in the relevant Service Schedule.

"**Services**" means the services specified in any Service Schedules that form part of this Agreement, including provision of the Output (to the extent available on relevant databases) and, where applicable, Documentation and Consultancy by TransUnion to the Client including, where agreed between the parties, access to TransUnion's Websites.

"**Service Conditions**" means, in respect of particular Services, the relevant additional terms and conditions described as Service Conditions in a Service Schedule and/or the Primary Schedule.

"Service Start Date" means (unless otherwise stated in the Primary Schedule) the earlier of (i) the date of commencement by TransUnion of, or the Client's use of (as the case may be), the Services falling within the scope of this Agreement (as logged by TransUnion's systems); and (ii) 30 days after the Agreement Signature Date.

"**Territory**" means the United Kingdom, or such other geographical area(s) that may be specified in this Agreement.

"**TransUnion**" means TransUnion International UK Limited or (where applicable) another member of the TransUnion Information Group that is involved in provision of the Services, as identified on the front page of this Agreement.

"**TransUnion's Websites**" means all and any areas of internet websites operated by TransUnion from time to time inaccessible to a public user.

"**TransUnion Information Group**" means TransUnion Information Group Limited (registered in England and Wales under company number 4968328) and its subsidiaries from time to time, including TransUnion.

"**Year**" means (i) in respect of the first Year, the period commencing on the Agreement Effective Date until the day before the Year 2 Start Date; and (ii) thereafter, each period of twelve consecutive months commencing on the Year 2 Start Date and each anniversary of that date.

"**Year 2 Start Date**" means (unless otherwise stated in the Primary Schedule) the first anniversary of the Service Start Date.

1.2 References to "**Primary Schedule**", "**Service Schedule**" and "**Payment Schedule**" shall mean those Schedules identified as such within this Agreement (where applicable), as listed on the front page of this Agreement.

1.3 The Schedules and their contents form part of this Agreement. The order of precedence shall be as described on the front page of this Agreement.

1.4 The headings in this Agreement are for convenience only and do not affect its interpretation.

1.5 A reference to a statute or statutory provision shall be construed as reference to it as from time to time amended, consolidated, modified, extended, re-enacted or replaced and includes all statutory instruments, notices or orders made under it.

1.6 References to clauses and Schedules are to the clauses and Schedules to this Agreement. References to paragraphs are to the paragraphs within the Schedules.

GENERAL TERMS FOR TRANSUNION SERVICES

(VERSION T39-OM1 10/25)

1.7 References to any gender includes all genders and the singular includes the plural and vice versa.

1.8 Any occurrence of the word “including”, “include” or “includes” shall be deemed to be followed by “without limitation” unless the context requires otherwise.

2 DURATION

2.1 This Agreement shall be deemed to have commenced on the Agreement Effective Date.

2.2 Subject to earlier termination in accordance with its terms, this Agreement shall continue for the duration specified in the Primary Schedule.

3 SUPPLY OF THE SERVICES AND INPUT

3.1 TransUnion warrants that it shall use reasonable care and skill in the provision of the Services.

3.2 As the Services are generic in nature and are provided as part of TransUnion’s standard service offering, TransUnion may, from time to time, change the form and content of the Services and/or (as the case may be) upgrade or modify any of the methods used to access the Services, including by way of a new minor version release. In such circumstances, TransUnion shall use reasonable endeavours that would be expected of a reputable business to give the Client not less than two months’ prior notice of any proposed material change, upgrade or modification and shall have due regard to the interests of the Client.

3.3 The Client shall ensure that it has the necessary facilities (including computer hardware, software and communications equipment) to obtain access to the Services.

3.4 For API deliveries (as identified within a Service Schedule), TransUnion only supports the current plus one previous Major Release of the API at any time (‘**Supported API**’). The Supported API includes any Minor Release within a Major Release. For the purpose of this clause 3.4, ‘**API**’ means the application programming interface (including the TransUnion Cosmos™ API) used to access TransUnion’s Services, ‘**Major Release**’ means v1.0, v2.0, v3.0 and so on, and ‘**Minor Release**’ means v1.1, v2.1, v3.1 and so on. The Client must operate a Supported API version. All new API versions, whether a Major Release or a Minor Release, must be implemented by the Client within six months of release by TransUnion (unless otherwise agreed in writing between the parties).

3.5 The Client shall provide the Input in the format agreed between the parties. If the Input is not received by TransUnion in that format, the Client will either promptly resubmit it in the agreed format or ask TransUnion to correct it at the Client’s expense (the charges for which shall be agreed between the parties).

3.6 The Client is responsible for the delivery of the Input to TransUnion, where this is required to enable provision of the Services.

3.7 The Client agrees to retain a copy of the Input so that TransUnion does not hold the Client’s only copy of the Input.

3.8 The Client acknowledges that it is not technically possible to guarantee uninterrupted access to Services provided over the internet. Accordingly, without prejudice to clause 3.1, TransUnion does not warrant or represent that the Services will be uninterrupted or continuously available.

3.9 TransUnion may, at its discretion, grant the Client access to one or more Services via TransUnion’s customer test site (“**CTest**”).

3.10 The Client acknowledges that CTest contains both fictitious data relating to fictitious individuals and personal data relating to real data subjects. Accordingly, Clause 8 of the General Terms shall apply to the Client’s use of the Services via CTest.

3.11 The Client agrees to comply with TransUnion’s rules and guidance on accessing CTest (as varied from time to time) (a copy of which shall be made available to the Client upon request).

3.12 Where the Client has been granted access to the Services via CTest, use of the Services via CTest, shall be limited to (i) application integration testing to test an API link; and/or (ii) testing the functionality of the Services within the CTest environment (as the case may be). Use of the Services via CTest for any other purpose, including any live, commercial purposes, is strictly prohibited.

4 DOCUMENTATION

4.1 Unless otherwise stated in a Service Schedule, where Documentation is made available to the Client pursuant to this Agreement, TransUnion grants to the Client a non-exclusive, non-transferable licence to use the Documentation, with effect from the Agreement Effective Date and for the duration of the licence of the Output contained in clause 5.1, for the sole purpose of enabling the Client to (i) receive any Online Service; or (ii) make use of the Output of any Consultancy, Batch Service, Portfolio Service or Data Management Service.

4.2 Subject to clause 12.6.2, the Client may make such number of copies of the Documentation made available to it under clause 4.1 as are necessary for the purpose described in clause 4.1, together with one copy of each for back-up and security purposes.

5 USE OF THE ONLINE SERVICES AND BATCH OUTPUT

5.1 Subject to clause 12, TransUnion:

5.1.1 licenses the Client to use the Online Services with effect from the relevant Service Start Date for the Online Services and for the duration of this Agreement for the Permitted Purpose only. The Client shall not use the Online Services for any other purposes whatsoever; and

5.1.2 grants to the Client a non-exclusive, non-transferable licence to use the Output of any Consultancy, Batch Service, Portfolio Service or Data Management Service for the Permitted Purpose only for a period of twelve months from the date of receipt thereof by the Client (or such other period as may be expressly stated in an applicable Service Schedule). The Client shall not use the Output of the Consultancy, Batch Service, Portfolio Service or Data Management Service for any other purposes whatsoever.

5.2 The Output cannot be used for any Prohibited Use.

5.3 The Client shall not sell, transfer, distribute, lease, charge or otherwise make the Services (including the Output) available to, or use the same on behalf of, any third party.

5.4 Where the Client accesses the Services (and/or receives the Output) via a third party appointed by the Client, the Client acknowledges that the third party is responsible for ensuring that any such Services (and/or Output) are not affected by the fact that the Services are utilised (or the Output is processed) via the third party and that TransUnion cannot be responsible for any defects or delay in the Services as a result of the Services being accessed via (or the Output being processed by) the third party rather than being accessed (or received) direct from TransUnion.

5.5 The Client warrants that it shall not be a Claims Management Company or carry out any activities analogous to those of Claims Management Company at any time during the term of this Agreement. Breach of this clause 5.5 shall be a material breach for the purposes of clause 12.4.1 of this Agreement.

5.6 The Client acknowledges and agrees that the data comprised within the Services and Output is based on information provided to TransUnion by third parties over whom TransUnion has no control. Therefore, TransUnion can give no warranties or representations as to the accuracy or the completeness of the Output.

5.7 TransUnion makes no warranties or representations as to the suitability of the Output for any particular purpose. Given the nature of the Services, TransUnion recommends that the Client does not use the Services as the sole basis for any business decision.

6 OWNERSHIP

6.1 All IPR in the Input (in the form received from the Client) shall at all times remain vested in the Client (or its third party licensors) and TransUnion shall acquire no rights in it save as expressly provided in this Agreement.

6.2 All IPR in the Output and the Services (excluding any part that is comprised of Input in the form received from the Client) shall at all times remain vested in TransUnion (or its third party licensors) and the Client shall acquire no rights in them save as expressly provided in this Agreement.

6.3 The Client grants to TransUnion a non-transferable, non-exclusive licence to use and copy the Input to enable TransUnion to provide the Services and to carry out its obligations under this Agreement.

6.4 The Client warrants that: (i) it has the right to license the Input to TransUnion for the purposes of this Agreement; and (ii) use of the Input pursuant to and in accordance with this Agreement, will not infringe the IPR of any third party.

6.5 Subject to clause 6.4, TransUnion warrants that it has the right to make the Output available to the Client for the purposes of this Agreement and has obtained the benefit of all necessary licences, consents and permissions that it is aware are necessary to facilitate this Agreement.

7 COMPLIANCE WITH LAWS

7.1 TransUnion and the Client shall at all times in respect of the subject matter of this Agreement comply with all Applicable Law including the Data Protection Legislation, the FSMA and the Regulations (as defined below).

7.2 The Client acknowledges that the supply of the Services by TransUnion and use thereof is governed by various statutes, regulatory requirements, codes of practice and guidelines relating to the use, provision and sharing of personal data and other information, including the Principles of Reciprocity (being the rules (as amended from time to time) established by the Steering Committee on Reciprocity which is an unincorporated body that governs the use of shared data in the credit industry), the regulatory policy, principles, codes and guidelines set down by the FCA and the ER Regulations (collectively “**the Regulations**”) and that the Regulations may change from time to time. The Client agrees that TransUnion may cease providing the whole or part of the Services if necessary in order to enable TransUnion to comply with the Regulations in which case TransUnion shall not be deemed to be in breach of this Agreement by reason of such cessation.

7.3 The Client is responsible for ensuring that it retains sufficient records and audits in respect of data utilised and searches made in respect of the Services as may be required by any regulator of the Client from time to time. Except as stated in the Service Conditions by express reference to this clause 7.3, TransUnion is not responsible for retaining such information.

8 SECURITY, SET UP, ADMINISTRATION AND DATA PROTECTION LEGISLATION

8.1 Each party shall comply with the Minimum Security Standards in place from time to time in respect of the subject matter of this Agreement.

8.2 Where the Client is granted access to TransUnion’s Websites it shall not access or attempt to access any part of TransUnion’s Websites that the Client does not have express authority to access.

8.3 Other than links to TransUnion’s privacy notices, the Client shall not carry out any linking of pages of any of TransUnion’s Websites, nor shall it incorporate any part of TransUnion’s Websites as part of the Client’s own website or that of any other party.

8.4 The Client agrees that it shall not (and it shall not engage any third party to) carry out any form of vulnerability assessment, penetration testing or load testing in respect of the Services or any of TransUnion’s Websites.

8.5 The Client is responsible for set up and administration of organisational structures, user IDs and passwords in relation to its use of the Services.

8.6 The Client shall provide details of all Client Users to TransUnion so that TransUnion can set up accounts for and issue user credentials to those Client Users to enable them to access the Services. The Client shall remain responsible for the actions of Client Users who have been issued with credentials until such time that a Client User's access has been disabled. For operational reasons (including user account lockouts, password resets and/or expirations due to lack of account activity), or for security reasons (including prevention of incidents and/or detection of irregular activity that may, if not acted upon, breach the security processes set up to protect the Services), TransUnion may change Client User credentials at any time.

8.7 The Client shall ensure that each Client User keeps their user credentials for the Services confidential. Client User credentials shall not be shared between individuals.

8.8 The Client agrees that use of the Services shall be limited to specialist operators for use in accordance with the Permitted Purpose, and that the Client shall therefore ensure that all Client Users have received appropriate training before they are allowed access to the Services. To the extent that TransUnion provides Documentation in respect of the Services, the Client shall include such Documentation as part of its Client User training programme.

8.9 The Client acknowledges that TransUnion acts as a controller in respect of any personal data contained within the Client User Data held by or on behalf of TransUnion. TransUnion shall process such personal data in accordance with the notice displayed on the TransUnion Website, at https://www.transunion.co.uk/legal/privacy-centre or such URL as is notified to the Client from time to time. The Client agrees to make the notice available to the Client Users in an appropriate manner so they are aware of TransUnion's processing of such data.

8.10 Each party shall comply with its obligations under the Data Protection Legislation in relation to any personal data processed in connection with this Agreement.

8.11 Without prejudice to clause 6.3, and save as provided in any Service Schedule, given TransUnion's significant degree of decision-making control and autonomy in determining the purposes and means by which the personal data (including the Input and Output) is processed pursuant to this Agreement, and decisions regarding the legal basis of any such processing, the parties acknowledge and agree that TransUnion acts as a controller (and not a processor) in relation to, and for the duration of, the processing of personal data, by it or any third party acting on its behalf, in connection with this Agreement.

8.12 As TransUnion has no direct relationship with the data subjects whose personal data is contained in the Input, in order for TransUnion to meet its transparency obligations under GDPR Article 14, it is a condition of the Client receiving the Services pursuant to this Agreement, that where, in accordance with this Agreement, TransUnion is acting as a controller in relation to the Input, the Client shall provide each data subject whose personal data is contained in the Input with access to the relevant TransUnion privacy notice as listed at https://www.transunion.co.uk/legal/privacy-centre. Details of which privacy notice should be used in relation to each TransUnion service are available from TransUnion on request.

8.13 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, each party shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk arising from its processing of personal data in connection with this Agreement, including as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. In assessing the appropriate level of security each party shall take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss or alteration of personal data and of unauthorised disclosure of, or access to, personal data.

8.14 To the extent that this Agreement expressly permits third parties to be given access to any personal data in the Output, the Client shall, before providing such access and periodically while such access persists, perform such due diligence checks on those third parties as are required in order to comply with good industry practice and Applicable Law. The Client shall not permit a third party to access the personal data if it does not satisfy, or ceases to satisfy, those checks.

9 CONFIDENTIALITY

9.1 Without prejudice to the provisions of clause 8 and subject to clause 9.3, each party shall in respect of the other party's Confidential Information:

9.1.1 keep it in strictest confidence and not make it available to any third party;

9.1.2 only use it for the purposes of this Agreement and ensure that only those of its employees who need to know have access to it; and

9.1.3 ensure that, before any employee is allowed access to it, the duty of confidentiality under this clause 9 is brought to such employee's attention.

9.2 Clause 9.1 survives the expiry or termination of this Agreement.

9.3 Clause 9.1 does not apply to Confidential Information to the extent that:

9.3.1 it is in the public domain at the date of its disclosure or subsequently comes in to the public domain otherwise than by breach of this Agreement;

9.3.2 the receiving party can show it was lawfully in its possession or known to it by being in its use or being recorded in its files or computers or other recording media before receipt from the disclosing party, or it has been lawfully developed by or for the receiving party independently of any Confidential Information disclosed to it by the disclosing party;

9.3.3 it was lawfully disclosed to the receiving party by any third party on a non-confidential basis and is not, to the receiving party's knowledge, the subject of any restriction as to its use or disclosure imposed by or on that third party at the time of provision;

9.3.4 the receiving party is obliged to disclose it by Applicable Law, by any court of competent jurisdiction or any regulatory body provided that (where permitted by Applicable Law) it gives the disclosing party reasonable notice of such disclosure and the reason for the disclosure;

9.3.5 provision of the Services requires TransUnion to make the Confidential Information available to sub-contractors, infrastructure providers or third party data suppliers who are subject to similar obligations of confidentiality; or

9.3.6 disclosure of the Confidential Information to third parties by the receiving party is permitted under the terms of this Agreement or has been authorised in writing by the disclosing party.

10 LIABILITY

10.1 Notwithstanding any other term of this Agreement neither party limits or excludes liability for fraud or fraudulent misrepresentation or for death or personal injury arising from its negligence. Clauses 10.2 to 10.9 (inclusive) are subject to this clause 10.1.

10.2 Neither party shall be liable for any special, indirect or consequential loss or damage arising out of or in connection with this Agreement or its subject matter (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise) even if that party had notice of the possibility of such loss.

10.3 Neither party shall be liable for any loss of business, loss of profits, loss of anticipated savings, loss of reputation, loss of goodwill, business interruption, increase in bad debt or any loss incurred by any third party arising out of or in connection with this Agreement or its subject matter (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise) even if that party had notice of the possibility of such loss.

10.4 The entire aggregate liability of each party in respect of all claims arising out of or in connection with this Agreement or its subject matter (other than, in respect of each party, those claims to which clauses 10.5 and 10.6 relate, and in the case of the Client, those claims to which clause 10.7 relates) in any Year (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise) shall not exceed an amount equal to (i) the sums received by or due to TransUnion from the Client under this Agreement during that Year; or (ii) £5,000, whichever is the greater.

10.5 The entire aggregate liability of each party in respect of all claims arising out of or in connection with its breach of (i) clause 7, (ii) clause 8; and/or (iii) clause 9 of this Agreement in any Year (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise) shall not exceed £1,000,000 (one million pounds sterling).

10.6 The entire aggregate liability of each party in respect of all claims arising out of or in connection with its breach of clause 6 of this Agreement in any Year (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise) shall not exceed £1,000,000 (one million pounds sterling).

10.7 Clauses 10.2 to 10.6 (inclusive) shall not limit or exclude the Client's liability in respect of any loss incurred arising out of or in connection with the Client's breach of clause 5 and the Client's entire liability in respect of such claims in any Year (whether arising in contract, tort (including negligence), breach of statutory duty or otherwise), shall not exceed £20,000,000 (twenty million pounds sterling).

10.8 Except as expressly provided in this Agreement, all conditions and warranties or terms of equivalent effect whether express or implied (by statute or otherwise) are excluded to the fullest extent permitted by Applicable Law.

10.9 The Client acknowledges that the Services may contain test data entries, details of which are available from TransUnion upon request. TransUnion excludes all liability that may arise from the granting of credit or the taking of other decisions in respect of individuals on the basis of the test data entries.

11 PAYMENT AND COSTS

11.1 The Client will pay TransUnion's charges for the Services as set out in the Payment Schedule within 30 days of the date of TransUnion's invoice.

11.2 All sums due under this Agreement must be paid in full without any set-off, counterclaim, deduction or withholding (other than any deduction or withholding of Applicable Tax which is required by law).

11.3 Subject to prior written consent from the Client (not to be unreasonably withheld or delayed), the Client shall reimburse TransUnion for those reasonable expenses incurred during performance of the Services by TransUnion's employees and consultants in accordance with TransUnion's expenses policy in place from time to time. Such expenses shall be invoiced to the Client monthly in arrears and shall be paid by the Client within 30 days of the date of TransUnion's invoice.

11.4 Any applicable value added, sales or other tax ("**Applicable Tax**") is to be paid by the Client at the prevailing rate on all sums due under this Agreement. All sums quoted in this Agreement are exclusive of any Applicable Tax.

11.5 Following the expiry of the first Year of this Agreement, TransUnion may increase the charges payable hereunder once in every Year during the continuance of this Agreement. Any such increase shall not exceed the increase (expressed as a percentage) in the Consumer Price Index since the later of the Agreement Signature Date or since the date of the last increase (if any) in TransUnion's charges. If the Consumer Price Index ceases to be published, then TransUnion and the Client shall agree another comparable replacement index (such agreement not to be unreasonably withheld or delayed).

12 SUSPENSION & TERMINATION

12.1 If, in relation to the Services, the Client breaches clause 5.1 or 5.3 of this Agreement or any other applicable licence restrictions under this Agreement, TransUnion may suspend the Services, including suspension of the licence to use any Output. For the avoidance of doubt, any such suspension pursuant to this clause 12.1 shall not affect the Client's obligations under clause 11.

12.2 Where any charges have not been paid in accordance with clause 11.1, or where fees are payable in advance of performance of the Services and such payment has not been made, TransUnion may suspend the performance of such Services until the relevant payment has been received.

12.3 TransUnion may also suspend the Services, including suspension of the licence to use any Output, in response to or in compliance with any law, statute, legislation, order, regulation or guidance issued by government, a court of law, an emergency service or any other competent regulatory authority or if the security processes set up to protect the Services are breached in any way.

12.4 Either TransUnion or the Client may terminate this Agreement and/or (regardless of this Agreement having already expired or terminated) any continuing licence under clause 5.1.2 immediately on notice if:

12.4.1 the other commits any material breach of this Agreement and such breach (where capable of remedy) is not remedied to the non-defaulting party's reasonable satisfaction within 14 days of notice specifying the breach and requiring its remedy;

12.4.2 in respect of the other, a resolution is passed or an order is made for winding up (save for the purpose of a bona fide reconstruction or amalgamation);

12.4.3 in respect of the other, an administration order is made, or a receiver or administrative receiver is appointed over any of its property or assets; or

12.4.4 the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts; or (being a company or limited liability partnership), is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 as if the words "it is proved to the satisfaction of the court" did not appear in sections 123(1)(e) or 123(2) of the Insolvency Act 1986; or (being an individual), is deemed either unable to pay its debts or as having no reasonable prospect of so doing, in either case, within the meaning of section 268 of the Insolvency Act 1986; or (being a partnership), has any partner to whom any of the foregoing apply.

12.5 On termination or expiry of this Agreement, TransUnion shall cease provision of the Services.

12.6 On termination or expiry of this Agreement or an applicable licence contained in clause 5.1 (whichever is the later) for whatever reason, the Client shall (subject to clause 12.8):

12.6.1 immediately cease using the Online Services and any Output;

12.6.2 promptly destroy, delete or return to TransUnion any Output, Documentation and any other materials provided by TransUnion relating to the Services (and all copies thereof) which remain in the possession or control of the Client; and

12.6.3 (upon request) provide TransUnion with a certificate of compliance with this clause 12.6 signed by a duly authorised officer.

12.7 Save where this Agreement is terminated by TransUnion pursuant to clause 12.4, the Client shall not be required to comply with clause 12.6 until the expiry or termination of the licence period applicable to the relevant Output.

12.8 Each party acknowledges that they may each have a standard data archiving policy which includes the creation and retention of backup copies of data and other information ("**Retained Data**") held on its computer systems for legal, regulatory compliance, IT restoration and disaster recovery purposes only. Each party agrees that the Retained Data held by the other party shall not be subject to an obligation to be returned or deleted, whether upon termination or expiry or otherwise. For the avoidance of doubt:

12.8.1 to the extent that the Retained Data are data and other information supplied to one party by the other party, it shall remain subject to the other terms of this Agreement as may be applicable; and

12.8.2 to the extent that the Retained Data are Output or information derived from it, such data may not be used by the Client for any live operational purposes (whether such use was within the scope of the Permitted Purpose or otherwise) after the date of termination or expiry of the applicable licence contained in clause 5.1.

12.9 TransUnion may terminate provision of any element of the Services (and the corresponding elements of the Output) immediately on notice in the event that TransUnion or its licensor ceases, for any reason, to have the right to make such Services and/or Output available. TransUnion shall not be deemed to be in breach of this Agreement and shall not have any liability to the Client in respect of such termination. In such circumstances, the parties agree to enter into good faith negotiations with a view to agreeing:

12.9.1 a pro rata refund of any charges paid in advance for the terminated Services in respect of any period after the date of termination to the extent that such Services have not yet been performed; and

12.9.2 an appropriate variation to the terms of this Agreement for provision of the unaffected Services.

12.10 On termination or expiry of this Agreement for any reason, any terms of this Agreement that either expressly or by their nature extend beyond the Agreement's termination remain in full force and effect. Without limiting the preceding sentence, the provisions of clauses 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and clauses 15 to 23 (inclusive) shall continue after termination or expiry of this Agreement in accordance with their terms.

13 AUDIT

13.1 Each party shall, subject to receipt of reasonable prior written notice from the other, permit a reasonable number of the other party's authorised employees and other representatives, including any competent regulatory authority, to have reasonable access during normal business hours to its relevant premises, documents and operations for the sole purpose of auditing compliance with this Agreement. The relevant premises, documents and operations are those which contain or might reasonably be expected to contain evidence of the host party's compliance or non-compliance with any term of this Agreement, but this clause does not entitle the visiting party to inspect any information which is (i) commercially sensitive, (ii) confidential for bona fide reasons of security or because of bona fide confidentiality obligations owed to a third party, or (iii) protected by legal privilege. The parties acknowledge that, where appropriate and agreed by the parties, audits and inspections under this clause 13.1 may be conducted virtually.

13.2 If either party exercises its right of audit under clause 13.1 it shall: (i) comply with the host party's reasonable safety and security rules and regulations in place from time to time; (ii) use reasonable endeavours to restrict its presence on the host party's premises to a maximum of two days; and (iii) reimburse the host party for all damage, losses, costs, claims demands and expenses suffered by the host party that are directly attributable to the visiting party's (or its authorised representatives') acts or omissions in exercising the right of audit.

14 FORCE MAJEURE

14.1 Neither party shall be liable to the other for any delay or non-performance of its obligations under this Agreement (except for its obligation to make payment) arising from any Event of Force Majeure.

14.2 The party affected by the Event of Force Majeure shall use reasonable endeavours to mitigate the impact of such Event of Force Majeure and to recommence performance of its obligations under this Agreement as soon as is reasonably practicable.

14.3 If the affected party is unable to perform its obligations under this Agreement by reason of the Event of Force Majeure for more than four weeks, the non-affected party may terminate this Agreement immediately by serving notice on the other and neither party shall be liable to the other by reason of such termination.

15 COUNTERPARTS, ELECTRONIC SIGNATURE AND VARIATION

15.1 This Agreement may be executed in any number of counterparts, all of which taken together will constitute one and the same agreement, and either party may enter into this Agreement by executing a counterpart.

15.2 This Agreement (and, where applicable, each counterpart) may be executed by electronic signature by any of the parties to any other party and the receiving party may rely on the receipt of such document so executed by electronic means as if the original had been received.

15.3 Any amendment, modification, variation or supplement to this Agreement (a "**Variation**") must be made in writing and signed by an authorised signatory of each party. References to the execution of this Agreement in clauses 15.1 and 15.2 shall also apply to the execution of any Variation to it.

16 ASSIGNMENT AND SUB-CONTRACTING

16.1 Either party is entitled to sub-contract the performance of any of its obligations under this Agreement provided that such party shall be liable for its obligations under this Agreement to the same extent as if it had carried out the work itself.

16.2 The Client shall not assign, transfer, charge or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of TransUnion (such consent not to be unreasonably withheld or delayed).

17 SEVERANCE

If any provision of this Agreement is found to be illegal or unenforceable by any court of competent jurisdiction then that provision shall be deemed to be deleted, but without affecting the remaining provisions.

18 AGENCY

Nothing in this Agreement constitutes a partnership between the parties. Neither party is deemed to be the agent of the other for any purpose and neither has the power or authority to bind the other or to contract in the name of the other.

19 ENTIRE AGREEMENT

19.1 This Agreement sets out the entire agreement between the parties in relation to its subject matter and supersedes all previous written or oral agreements, representations, understandings, warranties, conditions or arrangements between the parties in relation to that subject matter.

19.2 Each party acknowledges and agrees that in entering into this Agreement it has not relied on any statement, representation, assurance, condition or warranty (whether made negligently or innocently) other than as expressly set out in this Agreement.

19.3 Nothing in this clause 19 shall exclude or limit any liability of the parties arising as a result of any fraud or fraudulent misrepresentation.

20 WAIVER

Failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence is not to be construed as a waiver of that party's rights under this Agreement.

21 NOTICES

21.1 Any notice issued by the Client purporting to terminate this Agreement, whether in whole or in part, including any notice to terminate any Service Schedule or otherwise to terminate the right to receive services under this Agreement (in each case a "**Termination Notice**"), must be sent by email to the following address: UKContractTermination@transunion.com (or such other email address as is notified to the Client from time to time).

21.2 Save as set out in clause 21.1, all notices, requests, consents and authorisations given pursuant to this Agreement must be in writing and delivered by hand or sent by pre-paid first class mail, courier, Royal Mail Signed for 1st Class mail or Royal Mail Special Delivery Guaranteed mail and, where TransUnion is the recipient, be sent to its registered office address specified in the Primary Schedule (or such other address as is notified to the Client from time to time) and, where the Client is the recipient, be sent to its registered office or trading address as specified in the Primary Schedule (or such other trading address as is notified to TransUnion from time to time).

21.3 Subject to clause 21.5, any correctly addressed Termination Notice given pursuant to this Agreement shall be deemed to have been received at the time of transmission of the email containing the Termination Notice.

21.4 Subject to clause 21.5, any correctly addressed notices, requests, consents and authorisations given pursuant to this Agreement shall be deemed to have been received as follows:

21.4.1 if delivered by hand, on signature of a delivery receipt;

21.4.2 if sent by pre-paid first class mail, Royal Mail Signed for 1st Class or Royal Mail Special Delivery Guaranteed at 9.00am on the second day after posting;

21.4.3 if by courier, at the time recorded by the delivery service.

21.5 If deemed receipt under clauses 21.3 or 21.4 would occur outside Agreed Business Hours in the place of receipt, it shall be deferred until Agreed Business Hours first next resume. In this clause 21.5, "**Agreed Business Hours**" means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the United Kingdom.

21.6 The provisions of clauses 21.1 to 21.5 shall not apply to the service of any proceedings or other documents in any court, tribunal or other legal action or, where applicable, any arbitration, mediation or other method of dispute resolution facilitated by a third party

22 GOVERNING LAW AND JURISDICTION

22.1 The formation, existence, construction, performance, validity and all other aspects of this Agreement, any term of this Agreement and any non-contractual obligation undertaken or incurred in connection with this Agreement (including those arising out of pre-contractual dealings) will be governed by the laws of England.

22.2 The parties irrevocably agree that the courts of England shall have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in any way relate to this Agreement or its formation, existence, construction, performance, validity and any non-contractual obligation undertaken or incurred in connection with this Agreement (including those arising out of pre-contractual dealings) and, for these purposes, each party irrevocably submits to the exclusive jurisdiction of the courts of England.

22.3 The rights and remedies available to the parties in connection with this Agreement are cumulative and (except as otherwise stated) are not exclusive of any rights or remedies provided by law.

23 THIRD PARTY RIGHTS

23.1 Except as stated in the Service Conditions by express reference to this clause 23.1, a person who is not a party to this Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to rely on or enforce any term of this Agreement, but this does not affect any right or remedy of a third party which exists or is available apart from that Act.

23.2 Notwithstanding that any term of this Agreement may be or become enforceable by a person who is not a party to it, any of the terms of this Agreement may be varied, amended or modified or this Agreement may be suspended, cancelled or terminated by agreement in writing between the parties or this Agreement may be rescinded (in each case), without the consent of any such third party.

24 REFERENCE SITE AND CASE STUDY

24.1 TransUnion may publish the Client's name and logo, and information relating to the Services provided by TransUnion to the Client, in case studies, press releases, website content and other marketing materials provided that in each case TransUnion: (i) obtains the Client's prior written consent to any such proposed publication; and (ii) complies with any reasonable requirements specified in writing by the Client in relation to the publication, such as a requirement to comply with the Client's brand guidelines.