END USER CONSENT

SECURITY AND PRIVACY POLICIES

This document ("End User Consent and Policies") sets forth details of security and privacy standards and requirements that CA UMT Data Provider, Aggregator and every Approved Merchant must adhere to in respect of the provision of, receipt and use of the CA UMT Services. CA UMT Data Provider reserves the right, acting reasonably, to modify and/or augment this Schedule from time to time in the normal course of business and in particular as new CA UMT Services may be made available to Aggregator in the future. As used in this End User Consent and Policies, (i) "CA UMT Data Provider" means PersonMatch Utility Mobile Telco Data Provider in Canada; (ii) "Aggregator" means Trulioo Information Services Inc.; (iii) "CA UMT Services" means the Services provided by or through CA UMT Data Provider; (iv) "Approved Merchant" means Customer; and (v) "End User" means Consumers. Capitalized terms used and not otherwise defined in this End User Consent and Policies will have the meanings ascribed to such terms in the Agreement. This End User Consent and Policies shall only apply to Approved Merchant's use of CA UMT Services and will not otherwise affect the terms and conditions set out in the Agreement between End User and Aggregator. In the event of any inconsistency or conflict between the provisions of the Agreement and the End User Consent and Policies, the terms of End User Consent and Policies will prevail and govern only to the extent of such conflict and only in relation to the CA UMT Services.

1. **End User Consent**

Approved Merchant will, at all times obtain express consent from each End User (i)in accordance with all applicable Applicable Laws; and (ii) the basic requirements outlined below.

Basic requirements:

(a) The End User must have reached the age of majority according to the Applicable Laws of the jurisdiction where the End User resides.

(b) The request for consent made to the End User must include: (i) a description of the specific information being requested, (ii) a description of and how and under what circumstances it will be used (ie. its intended purpose), (iii) a description of the information provider(s) that explicitly includes “telecommunications service provider” or “mobile service provider”, and (iv) a statement confirming the End User’s consent to the information provider to disclose such information.

(c) Where consent from an End User is requested in an online or mobile application, Approved Merchant must have, as part of the mandatory transaction flow, an End User activated control that requires the End User to take a positive action to opt in, and which includes language substantially similar to the following: ***“By clicking the “Consent” or “Agree” button below, you expressly consent to us verifying and comparing your information (for ex. – first and last name, mobile phone number, etc.), account information (for ex. – account status, account type, etc.), location information (for ex. – latitude, longitude, etc.) to records of your information maintained by third parties including your telecommunications service provider(s) and you consent to such third parties providing such information to us or our third-party suppliers for the purpose of identity validation and/or performing a risk assessment.***

(d) Approved Merchant must provide or otherwise make available evidence of such End User Consent, in a form acceptable to CA UMT Data Provider, for each Query submitted to CA UMT Services, and maintain records of all such End User Consents for audit purposes. Approved Merchant acknowledges that if evidence of such End User Consent is not provided on request, CA UMT Data Provider may immediately cease providing CA UMT Services.

(e) Approved Merchant will not verify or attempt to verify any information about a End User prior to the End User's Consent having been obtained.

2. Privacy Controls

Approved Merchant acknowledges that Confidential Information, including Results and other Personal Information may be transmitted and as such, the security, availability, integrity and confidentiality of the Information is paramount to CA UMT Data Provider and Aggregator. Approved Merchant agrees to comply with all of the standard security practices and procedural requirements, to the extent applicable, as communicated from time to time, including without limitation the following security requirements:

(a) Put effective administrative, technological and physical safeguards in place to stop theft, loss and unauthorized access, copying, modification, use, disclosure or disposal of information that are consistent with industry best pratice;

(b) Educate its personnel with respect to applicable privacy laws and policies and take reasonable steps to ensure personnel compliance through staff training, confidentiality agreements and personnel sanctions, as needed;

(c) Ensure that employees who are fired or resign return all Information and cannot access applications, hardware, software, network and facilities belonging to either Aggregator, or CA UMT Data Provider as the case may be;

(d) Use tools like virus protection software, to avoid viruses, worms, back doors, trap doors, time bombs and other malicious software;

(e) Maintain backup security and acceptable business recovery plans (including disaster recovery, data backup and alternate power);

(f) Upon request, Approved Merchant will share its privacy policy with Aggregator or CA UMT Data Provider and provide any updates or changes made to its privacy policy during the term of the Agreement; and

(g) Upon request, Approved Merchant will permit representatives of Aggregator or CA UMT Data Provider to review the privacy policies and practices of Approved Merchant.

3. Security Controls

In addition to the obligations set out in Section 2 immediately above, Approved Merchant will:

(a) Implement information security policies, procedures, standards, guidelines and safeguards, normally within the context of an information security management system such as that defined in ISO/IEC 27001 to protect the security and confidentiality of all Confidential Information, including Result in compliance with the security, data and privacy requirements (including physical, technological and administrative measures) as set out herein;

(b) Perform background checks on employees performing the activities contemplated by this Agreement;

(c) Enforce access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities, etc.;

(d) Follow information security incident management procedures including mandatory incident reporting;

(e) Return or destroy all information received from Aggregator or CA UMT Data Provider, as the case may be, upon the termination or expiry of this Agreement;

(f) Conduct specification, design, development, testing, implementation, configuration, management, maintenance, support and use of security controls within or associated with IT systems;

(g) Use anti-malware, anti-spam and similar controls;

(h) Apply IT change and configuration management, including vulnerability management, patching and verification of system security controls prior to the connection to CA UMT Services;

(i) Have business continuity arrangements including crisis and incident management, resilience, backups and IT disaster recovery; and

(j) Provide reasonable co-operation to the Aggregator with respect to assisting Aggregator to resolve any incidents related to the activities contemplated in this Agreement, including co-operating with and assisting, to the extent it is permitted by law, administrative, regulatory or criminal processes, furnishing such information as may be reasonably required, and facilitating audits or site visits.