SCHEDULE C

Required Supplemental Terms and Conditions

This Schedule C (Required Supplemental Terms and Conditions) is fully incorporated by reference into your agreement(s) for screening services with RentGrow, Inc. (including through the Yardi® Breeze Terms of Use, if applicable) (each an "Agreement") and to the extent necessary replaces in its entirety all earlier revisions of these terms, however named, and whether contained in a Schedule C, an Exhibit 1, or that were otherwise part of the Agreement between you and RentGrow.



***NOTE**: For purposes of all TransUnion terms and conditions in this Schedule C only: (a) all references to "End User" shall mean and refer to Client, Property Manager and End-User as those terms are defined in the Agreement, as applicable; and (b) all references to "Subscriber" shall mean and refer to RentGrow as defined in the Agreement, as applicable.*

1. End User has a permissible purpose for obtaining consumer reports in accordance with the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) including, without limitation, all amendments thereto ("FCRA"). The End User certifies its permissible purpose as:
   - In connection with a credit transaction involving the consumer on whom the information is to be furnished an involving the extension of credit to, or review or collection of an account of the consumer; or
   - In connection with the underwriting of insurance involving the consumer or review of existing policy holders for insurance underwriting purposes, or in connection with an insurance claim where written permission of the consumer has been obtained; or
   - In connection with a tenant screening application involving the consumer; or
   - In accordance with the written instructions of the consumer; or
   - For a legitimate business need in connection with a business transaction that is initiated by the consumer; or
   - As a potential investor, servicer or current insurer in connection with a valuation of, or assessment of, the credit or prepayment risks.
2. End User certifies that End User shall use the consumer reports: (a) solely for the Subscriber's certified use(s); and (b) solely for End User's exclusive one-time use. End User shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with End User's own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by, and disclosed by End User only to End User's designated and authorized employees having a need to know and only to the extent necessary to enable End User to use the Consumer Reports in accordance with this Agreement. End User shall ensure that such designated and authorized employees shall not attempt to obtain any Consumer Reports on themselves, associates, or any other person except in the exercise of their official duties.
3. End User agrees that any of its computers from which a person could order, access, or view Consumer Reports are secured when unattended by authorized personnel who have a need to know the information contained in the Consumer Reports.
4. End User certifies that End User shall use any sex offender records delivered by Reseller within a consumer report only for the permitted purpose(s) certified by the End User and in accordance with all local state laws and regulatory restrictions that may restrict the use of sex offender records. Reseller agrees to ensure that End User is solely responsible for compliance with local state laws and regulations that may further limit the use of sex offender records within consumer reports.
5. THE FCRA PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18 OF THE UNITED STATES CODE OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.
6. End User shall use each Consumer Report only for a one-time use and shall hold the report in strict confidence, and not disclose it to any third parties; provided, however, that End User may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, unless otherwise explicitly authorized in an agreement between Reseller and its End User for scores obtained from TransUnion, or as explicitly otherwise authorized in advance and in writing by TransUnion through Reseller, End User shall not disclose to consumers or any third party, any or all such scores provided under such agreement, unless clearly required by law.
7. With just cause, such as violation of the terms of the End User's contract or a legal requirement, or a material change in existing legal requirements that adversely affects the End User's agreement, Reseller may, upon its election, discontinue serving the End User and cancel the agreement immediately.

Access to Information Contained in the Death Master File ("DMF")

End User certifies that it meets the qualifications of a Certified Person under 15 CFR Part 1110.2 and that its access to the DMF is appropriate because:

a. **Certified Person:** End User has a legitimate fraud prevention interest, or has a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty, and shall specify the basis for so certifying; and
b. **Security:** End User has systems, facilities, and procedures in place to safeguard the accessed information; experience in maintaining the confidentiality, security, and appropriate use of the accessed information, pursuant to requirements similar to the requirements of section 6103(p)(4) as if such section applied to End User; and
c. End User shall not disclose information derived from the DMF to the consumer or any third party, unless clearly required by law.
d. **Penalties:** End User acknowledges that failure to comply with the provisions above may subject Reseller to penalties under 15 CFR 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year.
e. **Indemnification and Hold Harmless:** End User shall indemnify and hold harmless TransUnion and the U.S. Government/NTIS from all claims, demands, damages, expenses, and losses, whether sounding in tort, contract, or otherwise, arising from or in connection with End User's, or End User's employees, contractors, or subcontractors, use of the DMF. This provision shall survive termination of the Agreement and will include any and all claims or liabilities arising from intellectual property rights.
f. **Liability:**
   a. Neither TransUnion nor the U.S. Government/NTIS (a) make any warranty, express or implied, with respect to information provided under this Section of the Policy, including, but not limited to, implied warranties of merchantability and fitness for any particular use; (b) assume any liability for any direct, indirect or consequential damages flowing from any use of any part of the DMF, including infringement of third party intellectual property rights; and (c) assume any liability for any errors or omissions in the DMF. The DMF does have inaccuracies and NTIS and the Social Security Administration, which provides the DMF to NTIS, does not guarantee the accuracy of the DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on the DMF is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the DMF.
   b. If an individual claims that SSA has incorrectly listed someone as deceased (or has incorrect dates/data on the DMF) the individual should be told to contact their local Social Security office (with proof) to have the error corrected. The local Social Security office will:
      i. Make the correction to the main NUMIDENT file at SSA and give the individual a verification document of SSA's current records to use to show any company, recipient/purchaser of the DMF that has the error; OR,
      ii. Find that SSA already has the correct information on the main NUMIDENT file and DMF (probably corrected sometime prior), and give the individual a verification document of SSA's records to use to show to any company subscriber/purchaser of the DMF that had the error.

TransUnion Scores

1. End User will request scores only for End User's exclusive use. End User may store Scores solely for End User's own use in furtherance of End User's original purpose for obtaining Scores. End User shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person except (i) to those employees of End User with a need to know and in the course of their employment; (ii) to those third party processing agents of End User who have executed an agreement that limits the use of the Scores by the third party to the use permitted to End User and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; or (iv) as required by law.

SCHEDULE C

Required Supplemental Terms and Conditions

***NOTE**: For purposes of all Equifax terms and conditions in this Schedule C only: (a) all references to "Qualified Subscriber" shall mean and refer to Client, Property Manager and End-User as those terms are defined in the Agreement, as applicable; and (b) all references to "CRA" shall mean and refer to RentGrow as defined in the Agreement, as applicable—except that the term "CRA" shall not define RentGrow as a consumer reporting agency for purposes of conferring on RentGrow any consumer reporting obligations as set forth in the FCRA when RentGrow is not subject to such obligations (such as when RentGrow is defined as a reseller as set forth in the FCRA).*

Equifax Information Services LLC ("Equifax")
Equifax Information Services (as defined below) will be received by Qualified Subscriber through CRA subject to the following conditions (the "Terms and Conditions"):

1. Any information services and data originating from Equifax (the "Equifax Information Services" or "Equifax Information") will be requested only for Subscriber's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted under the last sentence of this Paragraph. Only designated representatives of Qualified Subscriber will request Equifax Information Services on Qualified Subscriber's employees, and employees are forbidden to obtain consumer reports on themselves, associates or any other persons except in the exercise of their official duties. Qualified Subscriber will not disclose Equifax Information to the subject of the report except as permitted or required by law, but will refer the subject to Equifax.

2. Qualified Subscriber will hold Equifax and all its agents harmless on account of any expense or damage arising or resulting from the publishing or other disclosure of Equifax Information by Qualified Subscriber, its employees or agents contrary to the conditions of Paragraph 1 or applicable law.

3. Recognizing that information for the Equifax Information Services is secured by and through fallible human sources and that, for the fee charged, Equifax cannot be an insurer of the accuracy of the Equifax Information Services, Qualified Subscriber understands that the accuracy of any Equifax Information Service received by Qualified Subscriber is not guaranteed by Equifax, and Qualified Subscriber releases Equifax and its affiliate companies, agents, employees, and independent contractors from liability, even if caused by negligence, in connection with the Equifax Information Services and from any loss or expense suffered by Qualified Subscriber resulting directly or indirectly from Equifax Information.

4. Qualified Subscriber will be charged for the Equifax Information Services by CRA, which is responsible for paying Equifax for the Equifax Information Services.

5. Written notice by either party to the other will terminate these Terms and Conditions effective ten (10) days after the date of that notice, but the obligations and agreements set forth in Paragraphs 1, 2, 3, 6, 7, and 8 herein will remain in force.

6. Qualified Subscriber certifies that it will order Equifax Information Services that are consumer reports, as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FCRA"), only when Qualified Subscriber intends to use that consumer report information: (a) in accordance with the FCRA and all state law counterparts; and (b) for one of the following permissible purposes: (i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; (ii) in connection with the underwriting of insurance involving the consumer; (iii) as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; (iv) when Qualified Subscriber otherwise has a legitimate business need for the information either in connection with a business transaction that is initiated by the consumer, or to review an account to determine whether the consumer continues to meet the terms of the accounts; or (v) for employment purposes; provided, however, that QUALIFIED SUBSCRIBER IS NOT AUTHORIZED TO REQUEST OR RECEIVE CONSUMER REPORTS FOR EMPLOYMENT PURPOSES UNLESS QUALIFIED SUBSCRIBER HAS AGREED IN WRITING TO THE TERMS AND CONDITIONS OF THE EQUIFAX PERSONA SERVICE. Qualified Subscriber will comply with the applicable provisions of the FCRA, Federal Equal Credit Opportunity Act, Gramm-Leach-Bliley Act and any amendments to them, all state law counterparts of them, and all applicable regulations promulgated under any of them including, without limitation, any provisions requiring adverse action notification to the consumer. Qualified Subscriber will use each consumer report ordered under these Terms and Conditions for one of the foregoing purposes and for no other purpose.

7. It is recognized and understood that the FCRA provides that anyone "who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two (2) years, or both." Equifax may periodically conduct audits of Qualified Subscriber regarding its compliance with these Terms and Conditions, including, without limitation, the FCRA, other certifications and security provisions in these Terms and Conditions. Audits will be conducted by mail whenever possible and will require Qualified Subscriber to provide documentation as to permissible use of particular consumer reports. Qualified Subscriber gives its consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Qualified Subscriber's material breach of these Terms and Conditions, constitute grounds for immediate suspension of service or termination of these Terms and Conditions, notwithstanding Paragraph 5 above. If Equifax terminates these Terms and Conditions due to the conditions in the preceding sentence, Qualified Subscriber (i) unconditionally releases and agrees to hold Equifax harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and (ii) covenants it will not assert any claim or cause of action of any kind or nature against Equifax in connection with such termination.

8. California Law Certification. Qualified Subscriber will refer to Exhibit 1-A in making the following certification, and Qualified Subscriber agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act.
(QUALIFIED SUBSCRIBER'S AUTHORIZED REPRESENTATIVE MUST PLACE HIS/HER INITIALS NEXT TO THE APPLICABLE SPACE BELOW)

1. Do you, Qualified Subscriber certify you are a "retail seller," as defined in Section 1802.3 of the California Civil Code and referenced in Exhibit A1?
____ yes
_X_ no [your signature or other acknowledgment and acceptance of an Agreement with RentGrow (including through the Yardi® Breeze Terms of Use, if applicable) constitutes your initials here]

2. Do you, Qualified Subscriber issue credit to consumers who appear in person on the basis of an application for credit submitted in person?
____ yes
_X_ no [your signature or other acknowledgment and acceptance of an Agreement with RentGrow (including through the Yardi® Breeze Terms of Use, if applicable) constitutes your initials here]

[Exhibit 1-A - California Retail Seller: Provisions of the California Consumer Credit Reporting Agencies Act, as amended effective July 1, 1998, will impact the provision of consumer reports to Qualified Subscriber under the following circumstances: (a) if Qualified Subscriber is a "retail seller" (defined in part by California law as "a person engaged in the business of selling goods or services to retail buyers") and is selling to a "retail buyer" (defined as "a person who buys goods or obtains services from a retail seller in a retail installment sale and not principally for the purpose of resale") and a consumer about whom Qualified Subscriber is inquiring is applying, (b) in person, and (c) for credit. Under the foregoing circumstances, Equifax, before delivering a consumer report to Qualified Subscriber, must match at least three (3) items of a consumer's identification within the file maintained by Equifax with the information provided to Equifax by Qualified Subscriber in connection with the in-person credit transaction. Compliance with this law further includes Qualified Subscriber's inspection of the photo identification of each consumer who applies for in-person credit, mailing extensions of credit to consumers responding to a mail solicitation at specified addresses, taking special actions regarding a consumer's presentment of a police report regarding fraud, and acknowledging consumer demands for reinvestigations within certain time frames.

If Qualified Subscriber designated in Paragraph 8 of the Terms and Conditions that it is a "retail seller," Qualified Subscriber certifies that it will instruct its employees to inspect a photo identification of the consumer at the time an application is submitted in person. If Qualified Subscriber is not currently, but subsequently becomes a "retail seller," Qualified Subscriber agrees to provide written notice to Equifax prior to ordering credit reports in connection with an in-person credit transaction, and agrees to comply with the

requirements of the California law as outlined in this Exhibit, and with the specific certifications set forth herein.

Qualified Subscriber certifies that, as a "retail seller," it will either (a) acquire a new Qualified Subscriber number for use in processing consumer report inquiries that result from in-person credit applications covered by California law, with the understanding that all inquiries using this new Qualified Subscriber number will require that Qualified Subscriber supply at least three items of identifying information from the applicant; or (b) contact Qualified Subscriber's Equifax sales representative to ensure that Qualified Subscriber's existing number is properly coded for these transactions. **End of Exhibit 1-A]**

9. Vermont Certification. Qualified Subscriber certifies that it will comply with applicable provisions under Vermont law. In particular, Qualified Subscriber certifies that it will order information services relating to Vermont residents that are credit reports as defined by the Vermont Fair Credit Reporting Act ("VFCRA"), only after Qualified Subscriber has received prior consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Qualified Subscriber further certifies that the attached copy of Section 2480e (Exhibit 1-B) of the Vermont Fair Credit Reporting Statute was received from Equifax.

[Exhibit 1-B - Vermont Fair Credit Reporting Contract Certification
The undersigned, ("Qualified Subscriber"), acknowledges that it subscribes to receive various information services from Equifax Information Services LLC ("Equifax") in accordance with the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999), as amended (the "VFCRA") and the Federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. Seq., as amended (the "FCRA") and its other state law counterparts. In connection with Qualified Subscriber's continued use of Equifax information services in relation to Vermont consumers, Qualified Subscriber hereby certifies as follows:

Vermont Certification. Qualified Subscriber certifies that it will comply with applicable provisions under Vermont law. In particular, Qualified Subscriber certifies that it will order information services relating to Vermont residents, that are credit reports as defined by the VFCRA, only after Qualified Subscriber has received prior consumer consent in accordance with VFCRA § 2480e and applicable Vermont Rules. Qualified Subscriber further certifies that the attached copy of § 2480e of the Vermont Fair Credit Reporting Statute was received from Equifax. Qualified Subscriber: (please print)

Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999)
§ 2480e. Consumer consent
(a) A person shall not obtain the credit report of a consumer unless:

(1) the report is obtained in response to the order of a court having jurisdiction to issue such an order; or

(2) the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer.

(b) Credit reporting agencies shall adopt reasonable procedures to assure maximum possible compliance with subsection (a) of this section.

(c) Nothing in this section shall be construed to affect:

(1) the ability of a person who has secured the consent of the consumer pursuant to subdivision (a)(2) of this section to include in his or her request to the consumer permission to also obtain credit reports, in connection with the same transaction or extension of credit, for the purpose of reviewing the account, increasing the credit line on the account, for the purpose of taking collection action on the account, or for other legitimate purposes associated with the account; and

(2) the use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade Commission.

VERMONT RULES * CURRENT THROUGH JUNE 1999 *****
AGENCY 06. OFFICE OF THE ATTORNEY GENERAL
SUB-AGENCY 031. CONSUMER PROTECTION DIVISION
CHAPTER 012. Consumer Fraud--Fair Credit Reporting
RULE CF 112 FAIR CREDIT REPORTING
CVR 06-031-012, CF 112.03 (1999)
CF 112.03 CONSUMER CONSENT

(a) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing if the consumer has made a written application or written request for credit, insurance, employment, housing or governmental benefit. If the consumer has applied for or requested credit, insurance, employment, housing or governmental benefit in a manner other than in writing, then the person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing or in the same manner in which the consumer made the application or request. The terms of this rule apply whether the consumer or the person required to obtain consumer consent initiates the transaction.
(b) Consumer consent required pursuant to 9 V.S.A. §§ 2480e and 2480g shall be deemed to have been obtained in writing if, after a clear and adequate written disclosure of the circumstances under which a credit report or credit reports may be obtained and the purposes for which the credit report or credit reports may be obtained, the consumer indicates his or her consent by providing his or her signature.
(c) The fact that a clear and adequate written consent form is signed by the consumer after the consumer's credit report has been obtained pursuant to some other form of consent shall not affect the validity of the earlier consent. **End of Exhibit 1-B]**

10. Data Security.
10.1. This Paragraph 10 applies to any means through which Qualified Subscriber orders or accesses the Equifax Information Services including, without limitation, system-to-system, personal computer or the Internet.
For the purposes of this Paragraph 10, the term "Authorized User" means a Qualified Subscriber employee that Qualified Subscriber has authorized to order or access the Equifax Information Services and who is trained on Qualified Subscriber's obligations under these Terms and Conditions with respect to the ordering and use of the Equifax Information Services including Qualified Subscriber's FCRA and other obligations with respect to the access and use of consumer reports.

10.2. Qualified Subscriber will, with respect to handling Equifax Information:
(a) ensure that only Authorized Users can order or have access to the Equifax Credit Information;
(b) ensure that Authorized Users do not order consumer reports for personal reasons or provide them to any third party except as permitted by this Agreement;
(c) inform Authorized Users that unauthorized access to consumer reports may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment,
(d) ensure that all devices used by Qualified Subscriber to order or access the Equifax Credit Information are placed in a secure location and accessible only by Authorized Users, and that such devices are secured when not in use, through such means as screen locks, shutting power controls off, or other commercially reasonable security procedures;
(e) take all necessary measures to prevent unauthorized ordering of or access to the Equifax Credit Information by any person other than an Authorized User for permissible purposes, including, without limitation, limiting the knowledge of the Qualified Subscriber security codes, member numbers, User IDs, and any passwords Qualified Subscriber may use (collectively, "Security Information"), to those individuals with a need to know. In addition, the User IDs must be unique to each person, and the sharing of User IDs or passwords is prohibited,
(f) change Qualified Subscriber's user passwords at least every ninety (90) days, or sooner if an Authorized User is no longer responsible for accessing the Equifax Credit

Information, or if Qualified Subscriber suspects an unauthorized person has learned the password. Additionally, perform at least quarterly entitlement reviews to recertify and validate Authorized User's access privileges,
(g) adhere to all security features in the software and hardware Qualified Subscriber uses to order or access the Equifax Credit Information, including the use of IP restriction;
(h) implement secure authentication practices when providing User ID and passwords to Authorized Users, including but not limited to using individually assigned email addresses and not shared email accounts;
(i) in no event access the Equifax Credit Information via any hand-held wireless communication device, including, but not limited to, web enabled cell phones, interactive wireless pagers, personal digital assistants (PDAs), mobile data terminals and portable data terminals;
(j) not use non-company owned assets such as personal computer hard drives or portable and/or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs and DVDs) to store the Equifax Credit Information. In addition, Equifax Credit Information must be encrypted when it is not in use and all printed Equifax Credit Information, must be stored in a secure, locked container when not in use and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose;
(k) if Qualified Subscriber sends, transfers or ships any Equifax Credit Information, encrypt the Equifax Credit Information using minimum standards of Advanced Encryption Standard (AES), minimum 128-bit key, or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms, which standards may be modified from time to time by Equifax;
(l) not ship hardware or software between Qualified Subscriber's locations or to third parties without deleting all Security Information and any consumer information;
(m) monitor compliance with the obligations of this Section 8, and immediately notify Equifax if Qualified Subscriber suspects or knows of any unauthorized access or attempt to access the Equifax Credit Information, including, without limitation, a review of each Equifax invoice for the purpose of detecting any unauthorized activity,
(n) if, subject to Equifax approval, Qualified Subscriber uses a service provider to establish access to the Equifax Credit Information, be responsible for the service provider's use of Security Information, and ensure the service provider safeguards such Security Information through the use of security requirements that are no less stringent than those applicable to Qualified Subscriber under this Section 10;
(o) use commercially reasonable efforts to assure data security when disposing of any consumer report information or record obtained from Equifax. Such efforts must include the use of those procedures issued by the federal regulatory agency charged with oversight of Qualified Subscriber's activities (e.g. the Federal Trade Commission, the applicable banking or credit union regulator) applicable to the disposal of consumer report information or records.
(p) use commercially reasonable efforts to secure Equifax Credit Information when stored on servers, subject to the following requirements: (i) servers storing Equifax Credit Information must be separated from the Internet or other public networks by firewalls which are managed and configured to meet industry accepted best practices, (ii) protect Equifax Credit Information through multiple layers of network security, including but not limited to industry-recognized firewalls, routers, and intrusion detection/prevention devices (IDS/IPS), (iii) secure access (both physical and network) to systems storing Equifax Credit Information, which must include authentication and passwords that are changed at least every ninety (90) days, and (iii) all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available;
(q) not allow Equifax Information to be displayed via the Internet unless utilizing, at a minimum, a three-tier architecture configured in accordance with industry best practices;
(r) use commercially reasonable efforts to establish procedures and logging mechanisms for systems and networks that will allow tracking and analysis in the event there is a compromise, and maintain an audit trail history for at least three (3) months for review;
(s) provide immediate notification to Equifax of any change in address or office location and is subject to an onsite visit of the new location by Equifax or its designated representative, and;
(t) in the event Qualified Subscriber has a security incident involving Equifax Credit Information, Qualified Subscriber will fully cooperate with Equifax in a security assessment process and promptly remediate any finding.

11. These Terms and Conditions will be governed by and construed in accordance with the laws of the State of Georgia, without giving effect to its conflicts of laws provisions. These Terms and Conditions constitute the entire agreement of the parties with respect to Qualified Subscriber receiving Equifax Information Services and no changes in these Terms and Conditions may be made except in writing by an officer of Equifax.
_X_ Qualified Subscriber has read and understands these Terms and Conditions. [your signature or other acknowledgment and acceptance of an Agreement with RentGrow (including through the Yardi® Breeze Terms of Use, if applicable) constitutes your initials here]
_X_ Qualified Subscriber has read the attached "Notice to Users of Consumer Reports, Obligations of Users" which explains Qualified Subscriber's obligations under the FCRA as a user of consumer report information. [your signature or other acknowledgment and acceptance of an Agreement with RentGrow (including through the Yardi® Breeze Terms of Use, if applicable) constitutes your initials here]

12. Territory. Qualified Subscriber may access, use and store the Services and/or EVS Information only at or from locations within the territorial boundaries of the United States (the "Permitted Territory"). Qualified Subscriber may not access, use or store the Services and/or EVS Information at or from, or send it to any location outside of the Permitted Territory without first obtaining EVS's written permission.

Additional Equifax Information Services

If applicable, additional Equifax Information Services (as described below) will be received by Qualified Subscriber through CRA subject to the following conditions:

SAFESCAN® is an online warning systems containing information that can be used to detect possible fraudulent applications for credit. Some of the information in the SAFESCAN database is provided by credit grantors. SAFESCAN is a registered trademark of Equifax.

Permitted Use. SAFESCAN is not based on information in Equifax's consumer reporting database and is not intended to be used as a consumer report. Qualified Subscriber will not use a SAFESCAN alert or warning message in its decision-making process for denying credit or any other FCRA permissible purpose, but will use the message as an indication that the consumer's application information should be independently verified prior to a credit or other decision. Qualified Subscriber understands that the information supplied by SAFESCAN may or may not apply to the consumer about whom Qualified Subscriber has inquired.

SCHEDULE C

Required Supplemental Terms and Conditions



***NOTE**: For purposes of all Experian terms and conditions in this Schedule C only: (a) all references to "Third Party" shall mean and refer, as applicable, to Client, Property Manager and End-User as those terms are defined in the Agreement.*

Experian Security Requirements

The security requirements included in this document represent the minimum security requirements acceptable to Experian and are intended to ensure that a Third Party (i.e., Supplier, Reseller, Service Provider or any other organisation engaging with Experian) has appropriate controls in place to protect information and systems, including any information that it receives, processes, transfers, transmits, stores, delivers, and / or otherwise accesses on behalf of Experian

DEFINITIONS

"Experian Information" means Experian highly sensitive information including, by way of example and not limitation, data, databases, application software, software documentation, supporting process documents, operation process and procedures documentation, test plans, test cases, test scenarios, cyber incident reports, consumer information, financial records, employee records, and information about potential acquisitions, and such other information that is similar in nature or as mutually agreed in writing, the disclosure, alteration or destruction of which would cause serious damage to Experian's reputation, valuation, and / or provide a competitive disadvantage to Experian.

"Resource" means all Third-Party devices, including but not limited to laptops, PCs, routers, servers, and other computer systems that store, process, transfer, transmit, deliver, or otherwise access the Experian Information.

1. **Information Security Policies and Governance**
   Third Party shall have Information Security policies and procedures in place that are consistent with the practices described in an industry standard, such as ISO 27002 and / or this Security Requirements document, which is aligned to Experian's Information Security policy.

2. **Vulnerability Management**
   Firewalls, routers, servers, PCs, and all other resources managed by Third Party (including physical, on-premise or cloud hosted infrastructure) will be kept current with appropriate security specific system patches. Third Party will perform regular penetration tests to further assess the security of systems and resources. Third Party will use end-point computer malware detection / scanning services and procedures.

3. **Logging and Monitoring**
   Logging mechanisms will be in place sufficient to identify security incidents, establish individual accountability, and reconstruct events. Audit logs will be retained in a protected state (i.e., encrypted, or locked) with a process for periodic review.

4. **Network Security**
   Third Party will use security measures, including anti-virus software, to protect communications systems and networks device to reduce the risk of infiltration, hacking, access penetration by, or exposure to, an unauthorised third-party.

5. **Data Security**
   Third Party will use security measures, including encryption, to protect Experian provided data in storage and in transit to reduce the risk of exposure to unauthorised parties.

6. **Remote Access Connection Authorisation**
   All remote access connections to Third Party internal networks and / or computer systems will require authorisation with access control at the point of entry using multi-factor authentication. Such access will use secure channels, such as a Virtual Private Network (VPN).

7. **Incident Response**
   Processes and procedures will be established for responding to security violations and unusual or suspicious events and incidents. Third Party will report actual or suspected security violations or incidents that may affect Experian to Experian within twenty-four (24) hours of Third Party's confirmation of such violation or incident.

8. **Identification, Authentication and Authorisation**
   Each user of any Resource will have a uniquely assigned user ID to enable individual authentication and accountability. Access to privileged accounts will be restricted to those people who administer the Resource and individual accountability will be maintained. All default passwords (such as those from hardware or software vendors) will be changed immediately upon receipt.

9. **User Passwords and Accounts**
   All passwords will remain confidential and use 'strong' passwords that expire after a maximum of 90 calendar days. Accounts will automatically lockout after five (5) consecutive failed login attempts.

10. **Training and Awareness**
    Third Party shall require all Third Party personnel to participate in information security training and awareness sessions at least annually and establish proof of learning for all personnel.

11. **Experian's Right to Audit**
    Third Party shall be subject to remote and / or onsite assessments of its information security controls and compliance with these Security Requirements.

12. **Bulk Email Communications into Experian**
    Third party will not "bulk email" communications to multiple Experian employees without the prior written approval of Experian. Third party shall seek authorisation via their Experian Relationship Owner in advance of any such campaign.

SCHEDULE C

Required Supplemental Terms and Conditions



NOTE: *For purposes of all LexisNexis terms and conditions in this Schedule C only: (a) all references to "Customer" shall mean and refer to Client, Property Manager and End-User as those terms are defined in the Agreement, as applicable; and (b) all references to "Reseller" shall mean and refer to RentGrow as defined in the Agreement, as applicable.*

RESELLER AUDIT REQUIREMENTS

In addition to LexisNexis' own stringent security and audit programs, LexisNexis contractually requires its Resellers to have a defined audit program in place that will monitor Customers' usage, will be designed to reasonably prevent unauthorized usage, and will detect unauthorized or inappropriate use of LexisNexis data. Resellers must appropriately monitor Customers' use of the LexisNexis data and ensure Customers' compliance with the LexisNexis' standards, legal and regulatory obligations and contractual obligations made by Reseller to LexisNexis and by Reseller customers to the Reseller. Each Reseller's audit program must be designed to ensure compliance with, and meet the applicable requirements set forth in the GLBA, the FCRA, and the DPPA, as applicable. LexisNexis reserves the right to monitor and audit Reseller's Audit Program as it deems appropriate, in its sole discretion, and LexisNexis requires all Reseller's to cooperate fully and provide prompt responses to such monitoring and auditing. Violations, as determined by LexisNexis in its sole discretion, may be grounds for immediate changes without notice to account status, including but not limited to, suspension, change in service level provided, and/or termination of account.

CUSTOMER'S AUTHORIZATION OF AUDITS

By initialing below (your signature or other acknowledgment and acceptance of an Agreement with RentGrow (including through the Yardi® Breeze Terms of Use, if applicable) constitutes your initials here) Customer provides Reseller with express authorization to monitor its screening activity to ensure that Reseller is in compliance with its contract for LN Services, and that its Customers are in compliance with all laws and regulations. This will include random as well as regular monitoring of Customer activity to validate the permissible use of each search, including early detection of potentially fraudulent and/or suspicious activity.

GLBA DATA

Some of the information contained in the Reseller's Services is "nonpublic personal information," as defined in the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq. "GLBA"), and is regulated by the GLBA ("GLBA Data"). Customer shall not obtain and/or use GLBA Data through the Reseller's Services, in any manner that would violate the GLBA, or any similar state or local laws, regulations and rules. Customer acknowledges and agrees that it may be required to certify its permissible use of GLBA Data at the time it requests information in connection with certain Reseller Services. In addition, Customer agrees it will recertify, in writing, its permissible uses of GLBA Data upon request by Reseller. Customer certifies with respect to GLBA data received through the Reseller Services that it complies with the Interagency Standards for Safeguarding Customer Information pursuant to the GLBA.

DPPA DATA

Some of the information contained in the Reseller's Services is "personal information" as defined in the Driver's Privacy Protection Act (18 U.S.C. § 2721 et seq. "DPPA"), and is regulated by the DPPA ("DPPA Data"). Customer shall not obtain and/or use DPPA Data through the Reseller's Services in any manner that would violate the DPPA. Customer acknowledges and agrees that it may be required to certify its permissible use of DPPA Data at the time it requests information in connection with certain Reseller Services. In addition, Customer agrees it will recertify, in writing, to Reseller its permissible uses of DPPA Data upon the request of Reseller.

SCHEDULE C

Required Supplemental Terms and Conditions

***NOTE**: For purposes of all Contemporary Information Corporation ("CIC") terms and conditions in this Schedule C only: all references to "End User" shall mean and refer to Client, Property Manager and End-User as those terms are defined in the Agreement, as applicable.*

1. End User acknowledges and agrees that it will use public record data provided to RentGrow, Inc. and End User by CIC ("CIC Data") solely for the permissible purpose of evaluating applicants in connection with an application for a lease or rental of residential property, and End User will not request or use CIC Data for employment screening, employment pre-screening purposes, or any purpose prohibited by law.

2. End User consents to RentGrow providing CIC with the name, address, and phone number of any End User using CIC Data upon CIC's request.

3. End User represents and warrants that with each request for tenant screening information, including any requests for CIC Data, that End User has a permissible purpose pursuant to the FCRA for the information that is being requested and used. End User agrees to promptly provide RentGrow and CIC with proof of permissible purpose upon request, including a consumer's authorization (e.g., a copy of the original application).

4. End User represents and warrants that it is complying, and at all relevant times will remain in compliance, with all applicable federal, state and/or local laws, ordinances, statutes, and regulations which may apply to End User's business and its use of CIC Data, including the Vermont Fair Credit Reporting Statute (available here: https://legislature.vermont.gov/statutes/section/09/063/02480e) and the California Investigative Consumer Reporting Agency Act, as applicable.

5. End User agrees that CIC is not responsible for and expressly disclaims any responsibility for any scoring or decision models used, adopted, or otherwise implemented by End User that may implicate the use of CIC Data.

6. All CIC Data provided to End User shall be retained in strict confidence and disclosed only to those employees, agents, and/or independent contractors whose duties reasonably relate to legitimate business purposes for which information is requested, or as otherwise required by applicable law.

7. End User acknowledges that it has received a copy of CIC's Access Security Requirements from the website: https://www.cicreports.com/FCRA-Access-Security-Requirements-and-CIC-Policies. End User agrees to such requirements as may be modified by CIC from time to time and posted on that website. End User agrees that each time it places an order for CIC Data via the Internet, End User is, and will continue to be, in compliance with these requirements. If End User objects to changes required to the Access Security Requirements, End User may terminate the Agreement with RentGrow upon written notice. If End User continues to request services under the Agreement, then such requests shall be deemed End User's agreement to comply with such changes to the Access Security Requirements.

8. **END USER RECOGNIZES THAT UNLAWFUL DETAINER RECORDS, CRIMINAL RECORDS, AND OTHER DATA ARE SECURED FROM AND PROCESSED BY THIRD-PARTY SOURCES AND THAT, FOR THE FEE CHARGED, CIC CANNOT BE EITHER AN INSURER OR A GUARANTOR OF THE ACCURACY OF THE INFORMATION REPORTED. THUS, WHILE CIC WILL ADHERE TO THE STANDARD OF PERFORMANCE DETAILED IN ITS AGREEMENT WITH RENTGROW, INC., END USER ACKNOWLEDGES THAT CIC OBTAINS THE INFORMATION CONTAINED IN THE CIC DATA FROM THIRD PARTY SOURCES "AS IS," AND THEREFORE PROVIDES THE INFORMATION TO END USER ON AN "AS IS" AND "AS AVAILABLE" BASIS. EXCEPT AS OTHERWISE SET FORTH IN THESE TERMS AND CONDITIONS, CIC AND ITS DATA SOURCES AND PROVIDERS MAKE NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE, OR IMPLIED WARRANTIES ARISING FROM THE COURSE OF DEALING OR A COURSE OF PERFORMANCE, THAT THE CIC DATA WILL MEET END USERS' NEEDS, OR WILL BE PROVIDED ON AN UNINTERRUPTED BASIS; CIC EXPRESSLY DISCLAIMS ANY AND ALL SUCH REPRESENTATIONS AND WARRANTIES. EXCEPT AS EXPRESSLY SET FORTH IN THESE TERMS AND CONDITIONS, CIC, ON BEHALF OF ITSELF AND ITS DATA SOURCES AND PROVIDERS, EXPRESSLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE AND IMPLIED WARRANTIES ARISING FROM COURSE OF DEALING OR PERFORMANCE.**

SCHEDULE C

Required Supplemental Terms and Conditions



Additional Obligation(s):

Limited Access and Use of Information Obtained from the Social Security Administration's Database of Deceased Persons
The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("DMF"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1). As many credit bureau services contain information from the DMF, it is essential to restrict the use of deceased flags or similar indicia to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with applicable Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*) or Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq.*) use.

You acknowledge you will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other similar indicia within the services provided by the credit bureaus.

End User Required to Retain Consumer Authorizations
End-User will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.

End User Certification of No Further Sale
End User certifies that End User shall use the consumer reports: (a) solely for the Subscriber's certified use(s); and (b) solely for End User's exclusive one-time use. End User shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with End User's own data, or otherwise in any service which is derived from the consumer reports.

VantageScore℠ is a tri-bureau (TransUnion, Equifax and Experian) credit risk model developed using one algorithm across sample data common to all three credit bureaus. The following additional terms and conditions apply to receipt and use of VantageScore by Qualified Subscriber/Company/Customer ("Qualified Subscriber"):

End User Terms for VantageScore. Qualified Subscriber will request VantageScores only for Qualified Subscriber's exclusive use. Qualified Subscriber may store VantageScores solely for Qualified Subscriber's own use in furtherance of Qualified Subscriber's original purpose for obtaining VantageScores. Qualified Subscriber shall not use the VantageScores for model development or model calibration and shall not reverse engineer the VantageScore. All VantagScores provided hereunder will be held in strict confidence and may never be sold, licensed, copies, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any person except (1) to those employees of Qualified Subscriber with a need to know and in the course of their employment; (ii) to those third party processing agents of Qualified Subscriber who have executed an agreement that limits the use of the VantageScores by the third party only to the use permitted to Qualified Subscriber and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the VantageScore; or (iv) as required by law.

SCHEDULE C

Required Supplemental Terms and Conditions

NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's (CFPB) website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the Bureau's website. Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. Obligations of All Users of Consumer Reports

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

- As ordered by a court or federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Section 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state or local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5).

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term "adverse action" is defined very broadly by Section 603. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA – such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained from Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active Duty Military Alerts are in Files

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are available at www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

SCHEDULE C

Required Supplemental Terms and Conditions

II. Creditors Must Make Additional Disclosures

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations prescribed by the Consumer Financial Protection Bureau.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home Loan Applicant").

III. Obligations Of Users When Consumer Reports Are Obtained For Employment Purposes

A. Employment Other Than in the Trucking Industry

If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- Before taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of the consumer's rights. (The user should receive this summary from the CRA.). A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2).The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. Obligations When Investigative Consumer Reports Are Used

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subject of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure below.
- Upon written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. Special Procedures for Employee Investigations

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. Obligations Of Users Of Medical Information

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes - or in connection with a credit transaction (except as provided in federal regulations) - the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. Obligations Of Users Of "Prescreened" Lists

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Section 603(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. This statement must include the address and the toll-free telephone number of the appropriate notification system.
  In addition, once the CFPB has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The relevant regulation is 12 CFR 1022.54.

SCHEDULE C

Required Supplemental Terms and Conditions

VIII. Obligations of Resellers

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
  1) the identity of all end-users;
  2) certifications from all users of each purposes for which reports will be used; and
  3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. Liability For Violations Of The FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

The CFPB's website, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA. Citations for the FCRA sections in the U.S. Code, 15 U.S.C.§ 1681 et seq.:

Section 602 15 U.S.C. 1681
Section 603 15 U.S.C. 1681a
Section 604 15 U.S.C. 1681b
Section 605 15 U.S.C. 1681c
Section 605A 15 U.S.C. 1681cA
Section 605B 15 U.S.C. 1681cB
Section 606 15 U.S.C. 1681d
Section 607 15 U.S.C. 1681e
Section 608 15 U.S.C. 1681f
Section 609 15 U.S.C. 1681g
Section 610 15 U.S.C. 1681h
Section 611 15 U.S.C. 1681i
Section 612 15 U.S.C. 1681j
Section 613 15 U.S.C. 1681k
Section 614 15 U.S.C. 1681l
Section 615 15 U.S.C. 1681m
Section 616 15 U.S.C. 1681n
Section 617 15 U.S.C. 1681o
Section 618 15 U.S.C. 1681p
Section 619 15 U.S.C. 1681q
Section 620 15 U.S.C. 1681r
Section 621 15 U.S.C. 1681s
Section 622 15 U.S.C. 1681s-1
Section 623 15 U.S.C. 1681s-2
Section 624 15 U.S.C. 1681t
Section 625 15 U.S.C. 1681u
Section 626 15 U.S.C. 1681v
Section 627 15 U.S.C. 1681w
Section 628 15 U.S.C. 1681x
Section 629 15 U.S.C. 168

SCHEDULE C

Required Supplemental Terms and Conditions

California Report Certification

Pursuant to California Civil Code Sections 1786 – 1786.60 (the California Investigative Consumer Reporting Agency Act or "ICRAA"), as it exists and may be amended, Client certifies that as a user of the screening reports provided by RentGrow, Client is obtaining and using such reports solely for the permissible purpose of evaluating the qualification of rental applicants, reviewing the continuing qualification of tenants, or for some other permissible purpose as allowed by law and for no other purposes. Client further certifies that it has made and is solely responsible for making all ICRAA certifications applicable to users, including those described in paragraph (4) of subdivision (a) of Section 1786.16, and that Client shall comply with all other user obligations imposed under ICRAA.

SCHEDULE C

Required Supplemental Terms and Conditions

Secure Screening Report Access ("SSRA") Services Terms of Use

Version: April 25, 2025

These SSRA services Terms of Use, which will be updated from time to time (the "SSRA TOU"), are hereby incorporated into the Screening Services Activation Agreement (the "Agreement") that applies to the RentGrow tenant screening services you license from RentGrow, Inc. ("RentGrow"). You can access the most current version of the SSRA TOU online anytime here: http://www.rentgrow.com/us-screening-schedule-c.

For purposes of these SSRA TOU, "you", "your", "housing provider", "end-user", "user", "Client", and "Subscriber", all mean and refer to Client and End-User as defined in the Agreement, as applicable. Any capitalized terms used and not defined herein have the same meaning as defined in the Agreement.

This SSRA TOU shall apply to all Properties that use the RentGrow Services in any state (including but not limited to California and Colorado) where RentGrow has enabled the SSRA services, which RentGrow will enable from time to time, with or without notice. The SSRA services are designed to deliver to each Applicant who provides a valid email address when applying to any of your Properties in the applicable states that screen Applicants using the RentGrow Services a copy of the Applicant's tenant screening report, which is delivered via a secure link. In addition to delivering a copy of the Applicant's tenant screening report to the Applicant, the SSRA services include the ability for you to generate a report, at whatever time interval you choose, that indicates the name of the Applicant, whether their screening report was undeliverable to the email address provided by the Applicant, or whether their screening report was not deliverable because the Applicant did not provide an email address.

THE SSRA SERVICES ARE A TOOL TO HELP YOU MEET CERTAIN LEGAL OBLIGATIONS THAT, WHEN APPLICABLE, MAY REQUIRE YOU TO DELIVER TO YOUR APPLICANTS A COPY OF THEIR TENANT SCREENING REPORT. ONE SUCH EXAMPLE IS YOUR OBLIGATION UNDER CALIFORNIA LAW (NOT RENTGROW'S OBLIGATION) TO PROVIDE APPLICANTS WITH A "CHECK BOX" ON YOUR RENTAL APPLICATION FOR THE CONSUMER TO EXPRESSLY REQUEST A COPY OF THEIR SCREENING REPORT AND TO DELIVER A COPY OF THE SCREENING REPORT WITHIN THREE BUSINESS DAYS TO APPLICANTS THAT REQUEST IT AS REQUIRED UNDER CALIFORNIA'S INVESTIGATIVE CONSUMER REPORTING AGENCY ACT ("ICRAA").

THE REPORT COPY THAT IS DELIVERED TO AN APPLICANT BY THE SSRA SERVICES IS NOT INTENDED TO BE A PORTABLE OR REUSABLE TENANT SCREENING REPORT AS THESE TERMS ARE UNDERSTOOD, DEFINED, OR DESCRIBED IN CERTAIN JURISDICTIONS. THE REPORT COPY THAT IS DELIVERED IS INTENDED FOR THE CONSUMER AND REFLECTS THE SCREENING INFORMATION RENTGROW PROVIDED ABOUT THE CONSUMER TO THE SPECIFIC PROPERTY WHERE THE CONSUMER APPLIED.

RentGrow, as an Investigative Consumer Reporting Agency, as defined by California's ICRAA, has its own independent obligations under ICRAA. NOTHING ABOUT THE SSRA SERVICES, IN THESE SSRA TOU, OR IN YOUR AGREEMENT SHALL CREATE ANY LEGAL OBLIGATION THAT DOES NOT EXIST OR SHIFT ANY EXISTING LEGAL OBLIGATION FROM YOU TO RENTGROW, OR FROM RENTGROW TO YOU.

YOU, NOT RENTGROW, ARE RESPONSIBLE FOR MONITORING THE DELIVERY OF SCREENING REPORTS TO YOUR APPLICANTS, INCLUDING ANY OF YOUR DELIVERY OBLIGATIONS REQUIRED BY LAW. TO THE FULLEST EXTENT ALLOWED BY LAW, RENTGROW DISCLAIMS ALL WARRANTIES WITH REGARD TO THE SSRA SERVICES PROVIDED PURSUANT TO THESE SSRA TOU INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IF THE SSRA SERVICES DO NOT DELIVER A REPORT TO AN APPLICANT FOR ANY REASON, IT IS YOUR SOLE AND EXCLUSIVE OBLIGATION TO DO SO MANUALLY AND WITHIN ANY APPLICABLE TIME FRAME THAT MAY BE REQUIRED BY LAW.

IN THE EVENT OF ANY LOSS, CLAIM OR CAUSE OF ACTION ARISING OUT OF OR CONNECTED WITH YOUR FAILURE TO MONITOR THE DELIVERY OF REPORTS VIA THE SSRA SERVICE AND, IF NECESSARY, TO MANUALLY DELIVER SCREENING REPORTS TO YOUR APPLICANTS WITHIN ANY APPLICABLE TIME FRAME, RENTGROW SHALL HAVE NO LIABILITY TO YOU, REGARDLESS OF THE AMOUNT OF LOSS YOU MAY HAVE SUFFERED OR CLAIM TO HAVE SUFFERED, EXCEPT AS EXPRESSLY PERMITTED AND AS STRICTLY LIMITED BY THE TERMS OF YOUR AGREEMENT.

FOR THE AVOIDANCE OF DOUBT, IF, FOR ANY REASON, YOU QUESTION THE SUFFICIENCY OF THE SSRA SERVICES OR DETERMINE THAT THE SSRA SERVICES DO NOT MEET YOUR SPECIFIC NEEDS OR OBLIGATIONS, YOU MUST IMPLEMENT YOUR OWN INDEPENDENT PROCESS FOR DELIVERING SCREENING REPORTS TO YOUR TENANT APPLICANTS WHEN ANY SUCH OBLIGATION APPLIES TO YOU. DETERMINING WHETHER YOU HAVE SUCH AN OBLIGATION IS YOUR SOLE AND EXCLUSIVE RESPONSIBILITY. NOTHING IN THESE SSRA TOU, IN YOUR AGREEMENT, OR WITH THE SSRA SERVICES IS OR ARE INTENDED TO, NOR SHALL THEY, ALLEVIATE ANY OBLIGATION YOU HAVE UNDER THE LAW OR OTHERWISE, AND YOU AND YOUR LEGAL AND COMPLIANCE TEAMS SHOULD REGULARLY REVIEW, UNDERSTAND, AND COMPLY WITH ALL LAWS AND OBLIGATIONS THAT APPLY TO YOU AND YOUR PROPERTIES, WHEREVER THEY ARE LOCATED.

SCHEDULE C

Required Supplemental Terms and Conditions

SentiLink Synthetic Fraud Abuse Scores

For purposes of the terms and conditions related to the SentiLink Synthetic Fraud Abuse Scores ("Software") in this Schedule C only, all references to "End User" shall mean and refer to Client, Property Manager and End-User as those terms are defined in the Agreement.

1. End User Responsibilities. End User shall: (i) provide to SentiLink all information SentiLink determines, in its discretion, necessary to provide or furnish the Software in an electronic form and format approved by SentiLink ("End User Data"); (ii) use the Software in accordance with the Specifications; (iii) comply with law, rule, regulation, ordinance, code or order applicable to the acquisition, receipt or use of the Software and the procedures set forth in any other literature provided to End User by SentiLink; (iv) where required by applicable law, provide notices and obtain the written consent of, all End Users or Applicants that their information will be transferred or disclosed to Licensor for purposes described in this Schedule C; (iv) not use the Software in whole or in part, as a factor in determining eligibility for credit, insurance, or employment or for any other purpose contemplated by the Fair Credit Reporting Act ("FCRA"); and (v) not reverse engineer any Software or application programming interface provided by SentiLink.

2. By submitting End User Data to SentiLink, End User grants, and represents and warrants that it has all rights necessary to grant, all rights and licenses to the End User Data required to send the End User Data to SentiLink and for SentiLink and its subcontractors and service providers to provide the Software. SentiLink shall have no right to sublicense, sell, resell, or disclose to any third party the End User Data, except, however, that SentiLink and its subcontractors and services providers may collect, analyze, and use data derived from or part of the End User Data, solely for purposes of providing the Software, and analyzing, operating and improving SentiLink's fraud detection and prevention services.

3. End User certifies its use of the Software is solely for uses permitted by the GLBA, and to protect against or prevent actual fraud, unauthorized transactions, claims or other liability.

4. End User acknowledges that it will not take any adverse action against any consumer based solely on the information provided by SentiLink in the Software.

5. Intellectual Property. End User is not acquiring a copyright, patent or other intellectual property right in any Software, or in any data, modifications, customizations, enhancements, changes or work product related thereto.

6. End User hereby authorizes SentiLink to store and use all End User Data provided by or on behalf of End User and/or its customers in connection with the Software, and all information that is derived from such End User Data, in order to provide the Software, to create Depersonalized Information, to incorporate into its proprietary fraud prevention algorithms and models and fraud prevention services, and to disclose or use Depersonalized Information to enhance or improve SentiLink services or products or otherwise in order to prevent fraud, provided that (i) SentiLink cleanses such End User Data to remove End User's name and any NPI and otherwise renders such End User Data unidentifiable to any person, individual, consumer, or entity and not capable of being back-derived by an expert in the field using industry knowledge and available data-analytic tools and techniques (collectively, the "Depersonalized Information"), and (ii) the Depersonalized Information is included in a data set comprising both Depersonalized Information derived from End User Data and the Depersonalized Information derived from other SentiLink End Users ("Aggregate Form") such that the Depersonalized Information cannot be linked to End User. End User agrees that SentiLink is entitled to disclose such End User Data and derived information to third parties in order to facilitate its cleansing, provided that any such third parties are bound by commercially reasonable confidentiality and non-disclosure restrictions. SentiLink's rights with respect to Depersonalized Information or any data incorporated into its Services, including fraud prevention algorithms and models, under this provision shall survive the termination of the Agreement or any Service.

7. Indemnification. End User shall indemnify, defend and hold harmless SentiLink and its officers, employees, directors, agents, affiliates and shareholders, in their individual capacities or otherwise, (i) from and against any and all Claims asserted by an Applicant against SentiLink, and (ii) from and against any damages, costs, and expenses of such Applicant awarded against SentiLink by a final court judgment or an agreement settling such Claims in accordance with this Section 7. As used in this Section 7, the term "Claim" is limited to any action, litigation, or claim by an Applicant that result from, relate to, arise out of, or are incurred in connection with a failure to obtain all necessary consents and permissions from consumers whose personal information is being submitted to SentiLink. End User's obligation to indemnify SentiLink pursuant to this Section 6 shall not be deemed to limit any claim End User may have against SentiLink for breach of its obligations under the Agreement.

8. Disclaimer of Warranties. EXCEPT AS EXPRESSLY PROVIDED IN THESE GENERAL TERMS AND CONDITIONS OR AN ADDENDUM, SENTILINK DISCLAIMS ANY AND ALL WARRANTIES, CONDITIONS, OR REPRESENTATIONS (EXPRESS OR IMPLIED, ORAL OR WRITTEN) WITH RESPECT TO THE SOFTWARE, THIRD-PARTY SERVICES, DELIVERABLES, AND MATERIALS PROVIDED UNDER THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE, OR ERROR-FREE OPERATION (WHETHER OR NOT SENTILINK KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR IS OTHERWISE IN FACT AWARE OF ANY SUCH PURPOSE), WHETHER ALLEGED TO ARISE BY LAW, BY REASON OF CUSTOM OR USAGE IN THE TRADE, OR BY COURSE OF DEALING. IN ADDITION, SENTILINK DISCLAIMS ANY WARRANTY OR REPRESENTATION TO ANY PERSON OTHER THAN END USER WITH RESPECT TO THE SOFTWARE, THIRD-PARTY SERVICES, DELIVERABLES, EQUIPMENT, AND MATERIALS PROVIDED UNDER THIS AGREEMENT. END USER SHALL HAVE NO LIABILITY FOR ANY CLAIMS, LOSSES, OR DAMAGE CAUSED BY ERRORS OR OMISSIONS IN ANY INFORMATION PROVIDED TO SENTILINK BY END USER IN CONNECTION WITH THE DELIVERABLES OR SOFTWARE OR ANY ACTIONS TAKEN BY SENTILINK AT END USER'S DIRECTION. SENTILINK IS NOT A "CONSUMER REPORTING AGENCY," AS DEFINED BY THE FCRA AND THE DELIVERABLES AND SOFTWARE DO NOT CONSTITUTE A "CONSUMER REPORT," AS DEFINED BY FCRA AND SHALL NOT BE SUBJECT TO THE FCRA REQUIREMENTS RELATING TO DISPUTES, ACCESS, ACCURACY OR OTHERWISE.