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 he 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 valua ion 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 he purpose of selling, leasing, ren ing or otherwise providing information obtained under his Agreement to any other party, whe her 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 he Consumer Reports in accordance wi h 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 viola ion of he 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, discon inue 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 qualifica ions 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 informa ion 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 he 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 he 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 he third party to the use permitted to End User and contains the prohibitions set forth herein

regarding model development, model calibra ion and reverse engineering; (iii) when accompanied by the corresponding reason codes, to the consumer who is he subject of the Score; or (iv) as required by law.

SCHEDULE C

Required Supplemental Terms and Conditions

EQUIFAX®

***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 resul ing from he 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 Informa ion 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 Informa ion 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 cer ifies 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 whe her the consumer continues to meet the terms of he 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, cons itute 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) cons itutes 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) cons itutes your initials here]

[Exhibit 1-A - California Retail Seller: Provisions of the California Consumer Credit Reporting Agencies Act, as amended effec ive 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 hree (3) items of a consumer's identification within the file maintained by Equifax with he informa ion provided to Equifax by Qualified Subscriber in connection with the in-person credit transaction. Compliance with this law further includes Qualified Subscriber's inspec ion 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 reinvestiga ions 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 wi h the

requirements of he 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 he understanding hat 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 he 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 Repor ing 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 (he "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 wi h 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 his 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 he 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 wri ing 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 hird 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, shut ing 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 o her 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 hose 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 en itlement reviews to recertify and validate Au horized 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 Informa ion, including the use of IP restriction;
(h) implement secure authentica ion 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 he 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 loca ions or to third parties without deleting all Security Information and any consumer information;
(m) monitor compliance with the obligations of this Sec ion 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 Informa ion, 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 informa ion 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 wi h 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]

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 informa ion 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 indica ion 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 "Company" shall mean and refer to Client, Property Manager and End-User as those terms are defined in the Agreement, as applicable.*

Access Security Requirements for FCRA and GLB 5A Data

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to Experian systems or data, referred to as the "Company") responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. Experian reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security.

In accessing Experian's services, Company agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Experian data:

1. Implement Strong Access Control Measures

1.1 All credentials such as Subscriber Code number, Subscriber Code passwords, User names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Experian will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Experian's systems, ensure that the access must be preceded by authenticating users to the application and/or system (e g. application based authentication, Active Directory, etc.) u ilized for accessing Experian data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access Experian data/systems, is replaced or no longer in use, the passwords should be changed immediately.

1.4 Create a unique user ID for each user to enable individual authentication and accountability for access to Experian's infrastructure. Each user of the system access software must also have a unique logon password.

1.5 User IDs and passwords shall only be assigned to au horized individuals based on least privilege necessary to perform job responsibilities.

1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.

1.7 Develop strong passwords that are:

- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- For interac ive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.8 Passwords (e.g. subscriber code passwords, user password) must be changed immediately when:

- Any system access software is replaced by another system access software or is no longer used
- The hardware on which the software resides is upgraded, changed or disposed
- Any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements)

1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure hat strong encryption algorithms are utilized (e.g. AES 256 or above).

1.10 Implement password protected screensavers wi h a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

1.11 Active logins to credit information systems must be configured with a 30 minute inactive session timeout.

1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such informa ion are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.

1.13 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Experian data.

1.14 Ensure that Company employees do not access their own credit reports or those reports of any family member(s) or friend(s) unless it is in connec ion with a credit transaction or for another permissible purpose.

1.15 Implement a process to terminate access rights immediately for users who access Experian credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activi ies and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.18 Implement physical security controls to prevent unauthorized entry to Company's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. Maintain a Vulnerability Management Plan

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. An i-virus software deployed must be capable to detect, remove, and protect against all known types of malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that an i-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

3. Protect Data

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

3.2 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers,

servers, databases using strong encryption such as AES 256 or above.

3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protec ion and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

4. Maintain an Information Security Policy

4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable rules and regulations.

4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe Experian data may have been compromised, immediately notify Experian within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section*.

5. Build and Maintain a Secure Network

5.1 Protect Internet connection with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand-alone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

5.5 Change vendor defaults including but not limited to passwords, encryp ion keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access Experian systems, access to third party tools/services must require multi factor authentication.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to he issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data; establish a process for linking all access to such systems and applications. Ensure hat security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access credit reporting agency systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

- protecting against intrusions;
- securing the computer systems and network devices;
- and protecting against intrusions of operating systems or software.

7 Mobile and Cloud Technology

7.1 Storing Experian data on mobile devices is prohibited. Any excep ions must be obtained from Experian in writing; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

7.3 Mobile applica ions development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetrating testing) and ensuring vulnerabilities are remediated.

7.4 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

7.5 Mobile applica ions and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Experian data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

7.7 When using cloud providers to access, transmit, store, or process Experian data ensure that:

- Appropriate due diligence is conducted to maintain compliance wi h applicable laws and regulations and contractual obligations;
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
  - ISO 27001
  - PCI DSS
  - EI3PA
  - SSAE 16 – SOC 2 or SOC 3
  - FISMA

- CAI/CCM assessment

8 General

8.1 Experian may from time to time audit the security mechanisms Company maintains to safeguard access to Experian information, systems and electronic communica ions. Audits may include examination of systems security and associated administrative practices.

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to Experian upon request, audit trail information and management reports generated by the vendor software, regarding Company individual Authorized Users.

8.3 Company shall be responsible for and ensure that third party software, which accesses Experian information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

8.4 Company shall conduct software development (for software which accesses Experian information systems; this applies to both in-house or outsourced software development) based on the following requirements:

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

8.5 Reasonable access to audit trail reports of systems utilized to access Experian systems shall be made available to Experian upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to Experian must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Experian to Experian within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Experian of any confirmed security breach that may involve data related to the contractual rela ionship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800-295-4305, Email notification will be sent to regulatorycompliance@experian.com .

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Experian services, systems, or data, and (d) will abide by the provisions of these requirements when accessing Experian data.

8.9 Company understands that its use of Experian networking and computing resources may be monitored and audited by Experian, without further notice.

8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access Experian services or data are secure and in compliance with its membership agreement.

8.11 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by Experian.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 mon hs. In keeping with the ECOA, the credit reporting agency requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.

"Under Section 621(a)(2)(A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

Company certifies that it shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by Reseller; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Reseller, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information hat could result in substantial harm or inconvenience to any consumer.

Internet Delivery Security Requirements

In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Experian provided services via Internet ("Internet Access").

General Requirements

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Experian on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Experian provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such func ions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine he appropriate access to each Experian product based upon the legitimate business needs of each employee. Experian shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Experian. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). Experian's approval of requests for (Internet) access may be granted or wi hheld in its sole discretion. Experian may add to or change its requirements for gran ing (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*
4. An officer in the Company agrees to notify Experian in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

SCHEDULE C

Required Supplemental Terms and Conditions

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Experian on systems access and related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Experian on information and product access, in accordance with these Experian Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Experian's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Experian immediately.
2. As a Client to Experian's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Experian's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Experian representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.)
3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
4. Is responsible for ensuring that Company's Authorized Users are authorized to access Experian products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.
6. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Experian.
8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with Experian when needed on any system or user related matters.

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principal.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any participating network device – including routers, computers, time-servers, printers, Internet fax machines, and some telephones – must have its own its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information of the internet.
Subscriber Code	Your seven digit credit reporting agency account number.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an Annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA[SM] requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA[SM] also establishes quarterly scans of networks for vulnerabilities.
ISO 27001/27002	ISO 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard). The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16, SOC 2, SOC 3	Statement on Standards for Attestation Engagements (SSAE) No.1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report, just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law as part of the Electronic Government Act of 2002.
CAI/CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

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 he 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 wi h 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 ac ivity.

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, regula ions 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

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 he 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 Repor ing 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 o her 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 calibra ion 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 he 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 du ies 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 obliga ions 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. Sec ion 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 whe her 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. Sec ion 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valua ion or assessment of the credit or prepayment risks associated with an existing credit obligation. Sec ion 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 addi ion, 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

Sec ion 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 Sec ion 603. "Adverse actions" include all business, credit, and employment ac ions 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 for h 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 for h 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 Repor ing 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 he consumer his or her right to be told the nature of the informa ion that was relied upon if the consumer makes a written request wi hin 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 ac ion 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 wi h a nationwide consumer repor ing agency as defined in Sec ion 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer repor ing 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 he 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

Sec ion 605(h) requires nationwide CRAs, as defined in Section 603(p), to no ify users that request reports when the address for a consumer provided by the user in requesting he 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 regula ions 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 regula ions 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 for h in Sec ion 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 informa ion 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 for h 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 wri ing, 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 en ity 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 investiga ive consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an inves igative 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 Sec ion 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to he 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 Sec ion 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) - he consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical informa ion 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, hat 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 he 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 he 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 Cer ification 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 he 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) certifica ions 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

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.