RentTango

RENTTANGO.COM

CUSTOMER TERMS OF SERVICE AGREEMENT

The RentTango platform is intended to provide property managers and renters with innovative technology services to facilitate the leasing of residential real estate. It is our hope that the services available to you through our platform make the leasing experience enjoyable for your renters and easy for your leasing team.

This Terms of Service Agreement ("Agreement") sets forth the terms and conditions of the use of our online services by registered users (each, a "Customer") of RentTango.com ("RT" or "RentTango") for the purpose of advertising apartment and rental vacancies and processing rental applications (the "Services"). By using our Services, a Customer, or any other user of or visitor to our website, (together, "you") agree to these terms and conditions.

1. **User agreement.** In order to protect our users, as well as our information and service providers, you are required to comply with all of the rules set forth in this Agreement.

2. **Termination of service & billing errors**. You understand and agree that in RT's sole discretion, and without prior notice, RT may terminate your access to its Services, its websites, and its related applications, if any (together, the "Platform") and RT may also exercise any other available remedy. RT may also remove any unauthorized user content from the Platform if RT believes that your use of the Platform violates or conflicts with the Agreement, violates the rights of RT, or another user or the law. Claims for billing errors must be made in writing to RT within fifteen (15) days after date of invoice.

3. **Damages & relief against user.** You agree that monetary damages may not provide an adequate remedy to RT for violations of these terms and conditions. You therefore consent to injunctive or other equitable relief for such violations. RT is not required to provide any refund to you if this Agreement is terminated because you have violated this Agreement.

4. **Security for member account & password.** You are responsible for maintaining the confidentiality of any password(s) and account(s) registered to you. You are solely responsible for all activities that occur under your password(s) or account(s). You agree to immediately notify RT of any unauthorized use of your password(s) or account(s) or any other breach of security. You agree to make sure that you logout from your account(s) at the end of each session. RT cannot and will not be liable for any loss or damage arising from your failure to comply with this Section.

5. **Proprietary materials – restrictions on use.** All materials provided on the Platform, including but not limited to all text, logos, designs, graphics, images, sounds, information, software, documents, products and services, and the onsite selection, arrangement and display thereof, are the copyrighted works of RT and/or its vendors or suppliers. All materials herein and all RT software are the property of RT. Said materials and software are protected by worldwide copyright and/or other intellectual property laws. Unless provided for in this Agreement, none of said materials may be modified, copied, reproduced, distributed, republished, downloaded, displayed, sold, compiled, posted or transmitted in any form or by

any means. This ban includes, but is not limited to, electronic, mechanical, photocopying, recording or other means, without the prior express written permission of RT.

6. **Copyright and trademark information.** Except for content provided by the Customer, all content included or available on the Platform, including site design, text, graphics, interfaces, and the onsite selection and arrangements thereof is copyrighted by RT, with all rights reserved, or is the property of RT and/or third parties protected by intellectual property rights. Any use of materials on the Platform, including reproduction for purposes other than those noted above, modification, distribution, or replication, any form of data extraction or data mining, or other commercial exploitation of any kind, without prior written permission of an authorized officer of RT is strictly prohibited. Customer agrees that it will not use any automatic device (such as a "spider" or "robot" and/or any other automatic device) or any manual process to monitor or copy our web pages or the content contained therein without prior written permission of an authorized officer of RT. RT's trademarks may not be used in connection with any product or service that is not provided by RT, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits RT. All other trademarks displayed on RT's Platform are the trademarks of their respective owners. Their display does not constitute an endorsement or a recommendation of those vendors. In addition, such use of trademarks or links to the Platforms of vendors is not intended to imply, directly or indirectly, that those vendors endorse or have any affiliation with RT.

7. **Third-party sites and services.** For purposes of this Agreement, Customer acknowledges that RT may subcontract to third parties some aspects of the Services referenced herein. In the case of any subcontracted service, Customer agrees that all waivers, consents, indemnifications and any and all other terms contained herein shall be applicable to RT and/or any third party service provider, as the case may be. In addition to the foregoing, RT shall bear no responsibility for any acts of any third party service provider which are outside the control of RT. Any reference herein to RT that is, in practical effect, a reference to a third party service provider, shall not be deemed to impute any liability or duty of care to RT, its employees, officers, shareholders, successors and assigns, and/or agents. In addition, our Platform may include links to other sites on the Internet that are owned and operated by online merchants and other third parties. You acknowledge and understand that RT is not responsible for third-party sites and is not responsible for the availability or content of third-party sites. If you have any questions or concerns regarding such links or the content available on such sites, please contact your RT account manager. Your use of those third-party sites is subject to the terms of use and privacy policies of each third-party site. We are not responsible in any way for third-party sites. We encourage all Customers to review the privacy policies of third-parties' sites.

8. **Ban on resale of service.** You agree not to reproduce, duplicate, copy, sell, resell or exploit for any commercial purposes, any portion of the Services, use of the Services, or access to the Service.

9. **General disclaimer.** Although RT has attempted to provide accurate information on the Platform, RT assumes no responsibility for the accuracy of the information. You understand and agree that all information provided on this Platform is provided "as is," with all faults, without warranty of any kind, either express or implied. RT hereby disclaims all warranties, express or implied, including, and without limitation, those of merchantability, fitness for a particular purpose, title and non-infringement or arising from a course of dealing, and usage or trade practice. This is inapplicable where such a disclaimer has been legally held to be invalid but only to the extent of the specific invalidity.

10. **No unlawful or prohibited use.** As a condition of your use of the Services, you agree and represent to RT that you will comply with all applicable laws, statutes, ordinances and regulations regarding your use of the Services and any related activities. In addition, you agree and represent that you will not use the Services in any way prohibited by these terms, conditions and notices.

11. **Modification of the Platform.** RT reserves the right, in its sole discretion, to improve, modify or remove any information or content appearing on the Platform. Without prior notice, and in its sole discretion, RT may discontinue or revise any or all aspects of the Platform.

12. **Disclaimer regarding accuracy of vendor information.** Product specifications and other information have either been provided by the Vendors or collected from publicly available sources. While RT makes every effort to ensure that the information on this Platform is accurate, we can make no representations or warranties as to the accuracy or reliability of any information provided on this Platform.

13. **Governing jurisdiction of the courts of New York.** Our Platform is operated and provided in the State of New York. As such, we are subject to the laws of the state of New York. New York law will govern this Agreement, without giving effect to any choice of law rules. We make no representation that our Platform or other services are appropriate, legal or available for use in other locations. Accordingly, if you choose to access our site you agree to do so subject to the internal laws of the state of New York.

14. **Fair Housing Act.** As a Customer you agree not to take actions or make available content that violates the Fair Housing Act by stating, in any notice or ad for the sale or rental of any dwelling, a discriminatory preference based on race, color, national origin, religion, sex, familial status or handicap (or that otherwise violates any state or local law prohibiting discrimination on the basis of these or other characteristics.)

15. **Limitation of liability.** RT and its third party data suppliers shall not be liable for any damages whatsoever, and in particular RT and its third party data suppliers shall not be liable for any special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue, or loss of use, arising out of or in any way related to this Platform or the information contained in it, whether such damages arise in contract, negligence, tort, under statute, in equity, at law, or otherwise, even if RT or its third party data suppliers has been advised of the possibility of such damages. Limitation of Liability for e-commerce transactions: RT shall not be liable to any Customer or other user for the acts or omissions of any third party e-commerce provider when such acts or omissions negatively impact any transaction, or the transmission, reception, storage or handling of documents. RT shall not be liable for any indirect, incidental, special, consequential, punitive, or exemplary damages, including but not limited to, damages for loss of profits, revenue, goodwill, use, data, electronically submitted orders, or other economic advantage (even if it has been advised of the possibility of such damages), however caused and regardless of the theory of liability, arising out of or relates to (i) any delay, omission or error in the electronic transmission or receipt of any documents pursuant to this Agreement, or (ii) unauthorized access to or alteration by a third party of transmitted data.

16. **Possible exceptions to limitation of liability.** Because some jurisdictions do not allow for the limitation or exclusion of liability for incidental or consequential damages, some of the limitations set forth in the previous paragraph may be inapplicable.

17. **Indemnification.** You agree to indemnify and hold RT, its parents, subsidiaries, affiliates, third party data suppliers, officers and employees, harmless from any claim or demand, including reasonable attorneys' fees and costs, made by any third party due to or arising out of the Customer's use of the Services or any third party service, any violation of this Agreement, or infringement by a user of the Services using Customer's access, of any intellectual property or any other right of any person or entity. Such indemnification shall include violations, or actions by Customer which cause RT to be in violation, of any end-user license agreements or other third party agreements to which RT may be a party. You will also indemnify and hold us (including our affiliates and subsidiaries, as well as our and their respective officers, directors, employees, agents) harmless from any claim or demand, including reasonable legal fees, arising out of any e-commerce transaction, including but not limited to any damages for loss of profits, any technology malfunction, income, revenue, use, production, anticipated savings, business, contracts, commercial opportunities or goodwill. E-commerce is defined as the practice of buying and selling goods and services through online consumer services on the internet.

18. **Binding on assigns, successors and divested businesses.** Terms and agreements with RT will be binding upon and inure to the benefit of the parties and their assigns, successors and divested businesses. RT's agreement with Customer may not be transferred or assigned by Customer without the prior written consent of RT. "Successor" means any entity connected to a merger with Customer, sale of all or substantially all of the assets of Customer or other form of Customer's corporate reorganization. "Divested business" means any business unit that Customer sells, or of which it otherwise ceases to have an interest or render services. "Divested business" shall also include such business unit or the acquirer thereof, as applicable.

19. **Other terms.** If any provision of this Agreement shall be unlawful, void or unenforceable for any reason, the other provisions (and any partially-enforceable provision) shall not be affected thereby and shall remain valid and enforceable to the maximum possible extent. You agree that this Agreement and any other Agreements referenced herein may be assigned by RT, in our sole discretion, to a third party in the event of a merger or acquisition. This Agreement shall apply in addition to, and shall not be superseded by, any other written Agreement between us in relation to your participation as a Customer. Customer agrees that by accepting this Agreement, Customer is consenting to the use and disclosure of their personally identifiable information and other practices described in our Privacy Policy Statement. Customer may not assign, delegate, sub-contract or otherwise transfer this agreement (or any of its rights or obligations hereunder) without RT's prior written consent, and any attempt to do so without RT's approval will be void. RT may assign this agreement (or any of its rights or obligations hereunder) to a related company or to an unrelated company pursuant to a sale, merger of other consolidation of RT or any of its operating divisions upon written notice to Customer. Unless stated otherwise herein, "written notice" shall mean delivery by first class mail with a copy sent by email to the addresses for Customer on file with RT. Nothing in this Agreement is intended to confer any rights or remedies under or by reason of this Agreement on any person other than the parties and their respective successors and permitted assigns. The waiver by either party of a breach or violation of any provision of this Agreement shall not operate as, nor be construed to be, a waiver of any subsequent breach hereof. This Agreement may be amended only upon the RT's written consent. The terms that are defined

in this Agreement may be used in the singular or plural, or the masculine, feminine or neutral, as the context requires. The headings and subheadings in this Agreement are inserted for convenience of reference and shall not affect the meaning or interpretation of the Agreement.

20. Additional Restrictions Regarding Use of Marketing Services.

A. Content. Except for content provided by Customer, all content on the Platform designed by RT, whether artistic or technical in nature, shall be deemed to be owned by RT. Customer shall have a limited use of such content throughout the term of the Agreement for its intended use. Permission of RT is required for Customer to use such content other than the use intended by RT. RT may use any such content and usage statistics and testimonials, for its own promotional purposes. RT reserves the right to edit or reject advertising, photographs, artwork and copy provided by Customer and Customer accepts all liability for all content supplied by it. Customer warrants to RT that its copy is true, that it is not libelous or defamatory, that it violates no rights of privacy, that it infringes no trademark, copyright, literary or other rights, nor constitutes unfair competition with any other party, and that it complies with all federal, state and local laws and regulations, including any and all Fair Housing laws. The fact that content submitted to RT shall have been previously approved by it, either in whole or in part, shall not relieve the Customer of this warranty. Customer agrees to defend, indemnify, and hold harmless RT from any and all claims, demands, liability, suits, costs or expense, arising by reason of the publication of the Customer's consent, or breach of the foregoing warranty, whether such claims are well grounded or not.

B. No warranty. RT and its affiliates, agents and licensors, cannot and do not warrant the accuracy, completeness, currentness, non-infringement, merchantability or fitness for a particular purpose of the content designed by RT, whether artistic or technical, nor does RT guarantee that the content will be error-free, or continuously available, or that the Platform will be free of viruses or other harmful components. Under no circumstances will RT or its affiliates, agents or licensors be liable to Customer or anyone else for any damages, including, without limitation, consequential, special, incidental, indirect, punitive, exemplary, or other damages of any kind (including lost revenues or profits, loss of business or loss of data), even if RT is advised beforehand of the possibility of such damages. Customer agrees that the liability of RT and its affiliates, agents and licensors, if any, arising out of any kind of legal claim arising out of or otherwise related to this Agreement will not exceed the amount Customer paid, if any, to RT under the terms of this Agreement.

C. Fees imposed by third parties. RT's service rates and price schedule are independent of any fees imposed by other entities. If Customer requests a service of RT that results in the charging of additional fees, Customer thereby authorizes RT to contract for such services on Customer's behalf, and Customer is solely responsible for their payment.

21. Additional Restrictions and Terms of Use for Background Check Services. Use of RT's services is at Customer's sole risk. Customer acknowledges and agrees that while RT and its third-party data suppliers make every reasonable effort to assure that the data and information contained therein are an accurate reflection of the information received from their governmental and other sources, neither RT nor its third-party data suppliers can or does represent or warrant that the data and information contained therein or obtained therefrom will

be complete and accurate. Customer understands and agrees that its use of RT's services is entirely at its own risk. Neither RT nor its third-party data suppliers shall be liable or responsible for any inaccuracy of the data and information contained therein, or for interruption in service caused by the failure of the internet, by any act of God, or by any other force majeure. UNDER NO CIRCUMSTANCES SHALL RT OR ITS THIRD-PARTY DATA SUPPLIERS BE LIABLE FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY OR SPECIAL DAMAGES, INCLUDING LOST PROFITS, EVEN IF THEY HAVE BEEN MADE AWARE OF THE POTENTIAL FOR SUCH DAMAGES. ADDITIONALLY, RT AND ITS THIRD-PARTY DATA SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF CORRECTNESS, COMPLETENESS, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE DATABASES AND DATA AND INFORMATION CONTAINED THEREIN OR OBTAINED THEREFROM, OR SERVICES PROVIDED HEREUNDER.

A. **Parties will protect confidential information.** Both Customer and RT agree that they will, to the extent and in accordance with the policies used to protect its own information of similar importance, use their best efforts to refrain from and prevent the use of or disclosure of any confidential information as defined below ("Confidential Information") of the other party, disclosed or obtained by such party while performing its obligations under this Agreement, provided, however, that RT may disclose any information reasonably necessary to be disclosed in order for RT to provide the services and perform its obligations under this Agreement. Notwithstanding anything to the contrary, neither party shall use any Confidential Information in a manner which is detrimental to the other party. The phrase "Confidential Information" includes, without limitation, all materials and information supplied by one party to the other in the course of each party's performance under this Agreement, including but not limited to each party's business objectives and plans, marketing plans, customer lists, and financial information. Confidential Information includes, in addition to the information described above, reports, recommendations, scores, settings, any forms or agreements provided by RT to Customer, and any information available to Customer's internal platform. Neither party will have an obligation of confidentiality with regard to any information insofar as such information: (1) was known to such party prior to obtaining it from the other party; (2) is at the time of disclosure publicly available or becomes publicly available other than as a result of a breach of this Agreement; or (3) is disclosed to such Party by a third party not under a duty not to disclose such information.

B. **Transactions with third parties.** In the event that RT elects to enable direct transactions by applicants, whether through the Platform or an integrated third-party provider, RT agrees that these transactions will be charged using the same pricing model as the screening initiated by Customer via the RT interface. In the event RT elects to integrate third-party providers for related services, Customer grants RT permission to provide appropriate information for the purpose of generating such services, including but not limited to tenant data, applicant data, consumer reports and lease data. RT agrees to notify Customer in writing as soon as is practical upon termination of its relationship with any third-party to prevent unauthorized access of Customer's information.

C. **Limitations on document generation.** RT shall maintain an online collection of documents for Customer. Customer is solely responsible for the accuracy of its documents, will review documents produced by RT and will provide RT with any

changes or updates. ALL DOCUMENTS AND FORMS ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS.

D. **Price Adjustments.** Notwithstanding anything to the contrary in any Subscription Agreement submitted to Customer outlining the fees and services provided by RT, and/or any other agreement between Customer and RT, RT reserves the right to adjust the prices for certain services (including, but not limited to, fees for background check services provided hereunder) by providing written notice to Customer and the adjusted price will be effective on the date identified in the written notice (which may be provided, among other methods, via electronic mail to the address RT has on file for the Customer). Customer's continued acceptance of the service(s) for which the price was adjusted shall constitute Customer's agreement to be bound by the adjusted price. Customer may terminate the service(s) for which the price has been increased by providing written notice prior to such increase to RT, unless such price was increased due to an increase in charges to RT or its affiliate by any third party.

E. **Important Notice about the Death Master File.** Access to the Death Master File as issued by the Social Security Administration requires an entity to 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). The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("DMF"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1). As many of RT's services contain information from the DMF, we would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within our services to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with your applicable Fair Credit Reporting Act (15 U.S.C. §1681 et seq.) or Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) use. Your continued use of RT's services affirms your commitment to comply with these terms and all applicable laws. 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 indicia within RT's services.

F. **Customer will create a comprehensive security information program.** Customer 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 Customer's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the Customer by RT or any third party; 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 RT or any third party, (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 that could result in substantial harm or inconvenience to any consumer.

22. Fair Credit Reporting Act Requirements.

Although the federal Fair Credit Reporting Act (FCRA) and analogous state laws primarily regulate the operations of consumer credit reporting agencies, it also affects you as a user of information. You represent and warrant that you will comply with applicable laws and regulations, including, but not limited to, the FCRA, and RT shall bear no responsibility for such compliance.
You agree that you and your employees will review and become familiar with the FCRA, and with the following sections of the FCRA in particular:

§ 604. Permissible Purposes of Reports

§ 607. Compliance Procedures

§ 615. Requirement on users of consumer reports

§ 616. Civil liability for willful noncompliance

§ 617. Civil liability for negligent noncompliance

§ 619. Obtaining information under false pretenses

§ 621. Administrative Enforcement

§ 623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies

§ 628. Disposal of Records

Each of these sections is of direct consequence to users who obtain reports on consumers.

By law, consumer reports may be issued only if they are to be used for certain specific purposes. You agree that you will only request a report for a purpose that is permitted under the law and you understand that it is imperative that you identify each request for a report when such report is ordered. Additional state laws may also impact your usage of reports. 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. In addition to the FCRA, other federal and state laws addressing such topics as computer crime, unauthorized access to protected databases and use of personally identifiable information of individuals have also been enacted. You agree that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate.

23. **Privacy Policies.** The following information security controls are required to reduce unauthorized access to consumer information. These security controls shall supplement, not supplant, any and all local, state or federal rules, regulations and/or laws pertaining to the privacy and protection of consumer data and information including, but not limited to, any rules, regulations and/or laws analogous to the European Union's General Data Protection Regulation ("GDPR"). It is Customer's responsibility to implement these controls, and RT shall bear no responsibility for collecting, storing or protecting consumer information. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. RT reserves the right to make changes to these Privacy Policies without prior written notice. The information provided herewith provides minimum baselines for information security. In accessing RT's services, you agree to follow these security

requirements, which are applicable to all systems and devices used to access, transmit, process, or store credit bureau data:

A. <u>Implement strong access control measures</u>

i. All credentials such as User names/identifiers/account numbers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party.

ii. If using a third party or proprietary system to access **RT'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.) utilized for accessing **RT** data/systems.

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

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

v. User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.

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

vii. 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 eight (8) alpha/numeric characters for all user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

viii. Passwords (e.g. user/account 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)

ix. 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 that strong encryption algorithm are utilized (e.g. AES 256 or above).

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

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

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

xiii. Customer must not install Peer-to-Peer file sharing software on systems used to access, transmit or store credit bureau data.

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

xv. Implement a process to terminate access rights immediately for users who access credit bureau 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.

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

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

xviii. Implement physical security controls to prevent unauthorized entry to Customer'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.

B. <u>Maintain a vulnerability management program.</u>

i. Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.

ii. 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.

iii. 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. Anti-virus software deployed must be capable to detect, remove, and protect against all known types 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 anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

C. Protect data

i. 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, hard drive, paper, etc.).

ii. All credit reporting agency data is classified as confidential and must be secured to in accordance with this requirement at a minimum.

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

iv. Encrypt all credit bureau data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

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

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

vii. Applications utilized to access credit bureau data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

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

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

x. When no longer in use, electronic media containing credit bureau 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).

D. Maintain an information security policy

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

ii. 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 laws and regulations.

iii. 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 credit bureau data may have been compromised, immediately notify RT within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).

iv. The FACTA Disposal Rules requires that Customer 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.

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

E. Build and maintain a secure network

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

ii. 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.

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

iv. 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.

v. Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

vi. For wireless networks connected to or used for accessing or transmission of 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.

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

F. Regularly monitor and test networks

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

ii. Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit credit bureau data; establish a process for linking all access to such systems and applications. Ensure that 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 telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access **RT** 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.

G. Mobile and cloud technology

i. Storing credit bureau data on mobile devices is prohibited. Any exceptions must be obtained from the credit bureaus via **RT** in writing; additional security requirements will apply.

ii. 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.

iii. Mobile applications 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.

iv. 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.

v. Mobile applications 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 credit bureau data to be exchanged between secured and non-secured applications on the mobile device.

vi. In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing credit bureau 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.

vii. When using cloud providers to access, transmit, store, or process credit bureau data ensure that:

- Appropriate due diligence is conducted to maintain compliance with 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 the appropriate credit bureau:
    - ISO 27001
    - PCI DSS
    - EI3PA
    - SSAE 16 – SOC 2 or SOC3
    - FISMA
    - CAI / CCM assessment

H. General

i. **RT** may from time to time audit the security mechanisms Customer maintains to safeguard access to credit bureau information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices.

ii. In cases where the Customer is accessing credit bureau information and systems via third party software, the Customer agrees to make available to **RT** upon request, audit trail information and management reports generated by the vendor software, regarding Customer individual authorized users.

iii. Customer shall be responsible for and ensure that third party software, which accesses **RT** 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.

iv. Customer shall conduct software development (for software which accesses **RT** information systems; this applies to both in-house or outsourced software development) based on the following requirements:

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

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

vi. Data requests from Customer to **RT** must include the IP address of the device from which the request originated (i.e., the requesting Customer's IP address), where applicable.

vii. Customer shall report actual security violations or incidents that impact the credit bureaus to **RT** within twenty-four (24) hours or per agreed contractual notification timeline. Customer agrees to provide notice to **RT** of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 646.844.6483, or use the help chat function in the platform.

viii. Customer acknowledges and agrees that the Customer (a) has received a copy of these requirements, (b) has read and understands Customer'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 **RT** services, systems or data, and (d) will abide by the provisions of these requirements when accessing credit bureau data.

ix. Customer understands that its use of **RT** networking and computing resources may be monitored and audited by **RT**, without further notice.

x. Customer acknowledges and agrees that it is responsible for all activities of its employees/authorized users, and for assuring that mechanisms to access **RT** services or data are secure and in compliance with its Customership agreement.

xi. When using third party service providers to access, transmit, or store credit bureau data, additional documentation may be required by **RT**. ***Record Retention:*** *The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA,* ***RT*** *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*

breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency 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 $2,500 per violation."

24. **Internet Delivery Security Requirements.** In addition to the above, the following requirements apply where the Customer and its employees or an authorized agent/s acting on behalf of the Customer are provided access to RT's provided services via the internet ("Internet Access")

A. General requirements

i. The Customer shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with RT on systems access related matters. The Customer's Head Security Designate will be responsible for establishing, administering and monitoring all Customer employees' access to RT provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.

ii. The Customer'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 the appropriate access to each **RT** product based upon the legitimate business needs of each employee. **RT** shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.

iii. Unless automated means become available, the Customer shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by **RT**. 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). **RT's** approval of requests for (Internet) access may be granted or withheld in its sole discretion. **RT** may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Customer), 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.

iv. An officer of the Customer agrees to notify **RT** 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.

B. Roles and Responsibilities

i. Customer agrees to identify an employee it has designated to act on its behalf as a primary interface with **RT** on systems access 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 Customer and shall be available to interact with **RT** on information and product access, in accordance with these Access Security Requirements for FCRA and GLB 5A Data. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Customer. Customer's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Customer'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 **RT** systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to **RT** immediately.

ii. As a Customer to **RT's** products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Customer.

iii. The Security Designate may be appointed by the Head Security Designate as the individual that the Customer authorizes to act on behalf of the business in regards to **RT** product access control (e.g. request to add/change/remove access). The Customer can opt to appoint more than one Security Designate (e.g. for backup purposes). The Customer understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with **RT's** Security Administration group on information and product access matters.

iv. The Head Designate shall be responsible for notifying their corresponding **RT** 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.

C. Head Security Designate Requirements

i. Must be an employee and duly appointed representative of Customer, identified as an approval point for Customer's Authorized Users.

ii. Is responsible for the initial and on-going authentication and validation of Customer's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).

iii. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.

iv. Is responsible for ensuring that Customer's Authorized Users are authorized to access **RT** products and services.

v. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Customer.

vi. Must immediately report any suspicious or questionable activity to **RT** regarding access to **RT's** products and services.

vii. immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to **RT**.

viii. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.

ix. Shall be available to interact with **RT** when needed on any system or user related matters.

D. Changes to 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 **RT** systems and information.

25. Additional Rules on Background Screening. Customer hereby certifies that it will ensure that prior to procurement or causing the procurement of a consumer report that: (1) a clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report may be obtained; and (2) the consumer has authorized in writing the procurement of the report by Customer. In using a consumer report, before taking any adverse action based in whole or in part on the report, Customer shall provide to the consumer to whom the report relates: (1) a copy of the report; and (2) a description in writing of the rights of the consumer under FCRA in a format approved by the Federal Trade Commission. Customer requests for screening reports are pursuant to procedures prescribed by RT, are for a one-time use, and shall be held in strict confidence and not disclosed to any third parties not involved in the review. The information from the consumer report will not be used in violation of any applicable federal or state law or regulation. RT shall provide to Customer screening reports, and shall not provide general consumer reports or other services to any subscriber for such purpose. Customer shall provide to the consumer to whom the report relates a Summary of Consumer Rights as required by Section 609(c)(3) of FCRA with each report. By virtue of this certification, neither RT nor its data suppliers are providing legal advice to Customer regarding FCRA. These disclosures to the consumer include:

- Consumer must be told if information in your file has been used against him or her.
- Consumer has a right to know what is in his or her file, and this disclosure may be free. If a company relies on a consumer credit report and takes adverse action against consumer, consumer is entitled to receive a copy of that report from the company.
- Consumer has the right to ask for a credit score (there may be a fee for this service).

- Consumer has the right to dispute incomplete or inaccurate information. Consumer reporting agencies must correct or delete inaccurate, incomplete or unverifiable information.
- Access to your file is limited. Consumer must get permission for reports to be furnished to background screeners.

  A summary of consumer rights under the Fair Credit Reporting Act are available by visiting or writing: (Para informacion en espanol, visite o escribe:) https://www.ftc.gov/credit or Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580

26. RESERVED

27. Additional rules governing FICO scores from TransUnion

Based on an agreement with TransUnion and Fair Isaac Corporation (Fair Isaac), RT has access to a unique and proprietary statistical credit scoring service jointly offered by TransUnion and Fair Isaac which evaluates certain information in the credit reports of individual consumers from TransUnion's database (Classic) and provides a score (the Classic Score). Customer may desire to obtain Classic Scores from TransUnion in connection with consumer credit reports. Customer will request Scores only for Customer's exclusive use and may store Scores solely for Customer's own use in furtherance of Customer's original purpose for obtaining the Scores. Customer has a permissible purpose for obtaining consumer reports, as defined by Section 604 of FCRA. Customer shall not use the Score for model development or model calibration and shall not reverse-engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part to any Person except (i) to those employees of Customer with a need to know and in the course of their employment; (ii) to those third party processing agents of Customer who have executed an agreement that limits the use of the Scores by the third party to the use permitted to Customer and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; or (iv) as required by law. Customer recognizes that factors other than the Classic Score may be considered in making a credit decision. Such other factors include, but are not limited to, the credit report, the individual account history, and economic factors. TransUnion and Fair Isaac shall be deemed third party beneficiaries under this clause. Up to five score reason codes, or if applicable, exclusion reasons, are provided to Customer with Classic Scores. These score reason codes are designed to indicate the reasons why the individual did not have a higher Classic Score, and may be disclosed to consumers as the reasons for taking adverse action, as required by the Equal Credit Opportunity Act (ECOA) and its implementing Regulation (Reg. B). However, the Classic Score itself is proprietary to Fair Isaac, may not be used as the reason for adverse action under Reg. B and, accordingly, shall not be disclosed to credit applicants or any other third party, except: (1) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (2) as clearly required by law. Customer will not publicly disseminate any results of the validations or other reports derived from the Classic Scores without Fair Isaac and TransUnion's prior written consent. In the event Customer intends to provide Classic Scores to any agent, Customer may do so provided, however, that Customer first enters into a written agreement with such agent that is consistent with Customer's obligations

under this agreement. Moreover, such agreement between Customer and such agent shall contain the following obligations and acknowledgments of the agent: (1) Such agent shall utilize the Classic Scores for the sole benefit of Customer and shall not utilize the Classic Scores for any other purpose including for such agent's own purposes or benefit; (2) That the Classic Score is proprietary to Fair Isaac and, accordingly, shall not be disclosed to the credit applicant or any third party without TransUnion and Fair Isaac's prior written consent except (a) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (b) as clearly required by law; (3) Such Agent shall not use the Classic Scores for model development, model validation, model benchmarking, reverse engineering, or model calibration; (4) Such agent shall not resell the Classic Scores; and (5) Such agent shall not use the Classic Scores to create or maintain a database for itself or otherwise. Customer acknowledges that the Classic Scores provided under this Agreement which utilize an individual's consumer credit information will result in an inquiry being added to the consumer's credit file. Customer shall be responsible for compliance with all applicable federal or state legislation, regulations and judicial actions, as now or as may become effective including, but not limited to, the FCRA, the ECOA, and Reg. B, to which it is subject. Fair Isaac, the developer of Classic, warrants that the scoring algorithms as delivered to TransUnion and used in the computation of the Classic Score (Models) are empirically derived from TransUnion's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring when applied to the population for which they were developed, and that no scoring algorithm used by Classic uses a "prohibited basis" as that term is defined in the ECOA) and Reg. B promulgated thereunder. Classic provides a statistical evaluation of certain information in TransUnion's files on a particular individual, and the Classic Score indicates the relative likelihood that the consumer will repay their existing or future credit obligations satisfactorily over the twenty-four (24) month period following scoring relative to other individuals in TransUnion's database. The score may appear on a credit report for convenience only, but is not a part of the credit report nor does it add to the information in the report on which it is based. THE WARRANTIES SET FORTH ARE THE SOLE WARRANTIES MADE UNDER THIS CLAUSE CONCERNING THE CLASSIC SCORES AND ANY OTHER DOCUMENTATION OR OTHER DELIVERABLES AND SERVICES PROVIDED UNDER THIS AGREEMENT; AND NEITHER FAIR ISAAC NOR TRANSUNION MAKE ANY OTHER REPRESENTATIONS OR WARRANTIES CONCERNING THE PRODUCTS AND SERVICES TO BE PROVIDED UNDER THIS AGREEMENT OTHER THAN AS SET FORTH HERE. THE WARRANTIES AND REMEDIES SET FORTH ABOVE ARE IN LIEU OF ALL OTHERS, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPRTE. IN NO EVENT SHALL ANY PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES INCURRED BY THE OTHER PARTIES AND ARISING OUT OF THE PERFORMANCE OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LRTS OF GOOD WILL AND LRTT PROFITS OR REVENUE, WHETHER OR NOT SUCH LRTS OR DAMAGE IS BASED IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY, OR OTHERWISE, EVEN IF A PARTY HAS BEEN ADVISED OF THE PRTSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPRTE OF ANY LIMITED REMEDY. THE FOREGOING NOTWITHSTANDING, WITH RESPECT TO CUSTOMER, IN NO EVENT SHALL THE AFORESTATED LIMITATIONS OF LIABILITY, SET FORTH ABOVE

IN SECTION 16, APPLY TO DAMAGES INCURRED BY TRANSUNION AND/OR FAIR ISAAC AS A RESULT OF: (A) GOVERNMENTAL, REGULATORY OR JUDICIAL ACTION(S) PERTAINING TO VIOLATIONS OF THE FCRA AND/OR OTHER LAWS, REGULATIONS AND/OR JUDICIAL ACTIONS TO THE EXTENT SUCH DAMAGES RESULT FROM CUSTOMER'S BREACH, DIRECTLY OR THROUGH CUSTOMER'S AGENT(S), OF ITS OBLIGATIONS UNDER THIS AGREEMENT. ADDITIONALLY, NEITHER TRANSUNION NOR FAIR ISAAC SHALL BE LIABLE FOR ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS ADDENDUM BROUGHT MORE THAN ONE (1) YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED. IN NO EVENT SHALL TRANSUNION'S AND FAIR ISAAC'S AGGREGATE TOTAL LIABILITY, IF ANY, UNDER THIS AGREEMENT, EXCEED THE AGGREGATE AMOUNT PAID, UNDER THIS ADDENDUM, BY CUSTOMER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING ANY SUCH CLAIM, OR TEN THOUSAND DOLLARS ($10,000.00), WHICHEVER AMOUNT IS LESS. This Agreement may be terminated automatically and without notice: (1) in the event of a breach of the provisions of this supplement by Customer; (2) in the event the agreement(s) related to Classic between TransUnion, Fair Isaac and RT are terminated or expire; (3) in the event the requirements of any law, regulation or judicial action are not met, (4) as a result of changes in laws, regulations or regulatory or judicial action, that the requirements of any law, regulation or judicial action will not be met; and/or (5) the use of the Classic Service is the subject of litigation or threatened litigation by any governmental entity.

28. <u>Additional Rules on California Retail Sellers</u>

California Civil Code – Section 1785.14(a)Section 1785.14(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met: Section 1785.14(a)(1) states: "If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name. "Section 1785.14(a)(2) states: "If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller must certify, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail. "Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed." In compliance with Section 1785.14(a) of the California Civil Code, Customer hereby certifies to RT Customer is NOT a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale"). End User also certifies that if End User is a Retail Seller who conducts Point of Sale transactions, End User will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person. End User also

certifies that it will only use the appropriate End User code number designated by Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller. If End User is not a Retail Seller who issues credit in Point of Sale transactions, End User agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, End User shall provide written notice of such to Consumer Reporting Agency prior to using credit reports with Point of Sale transactions as a Retail Seller, and shall comply with the requirements of a Retail Seller conducting Point of Sale transactions, as provided in this certification.

29. Additional Rules on Vermont Consumers

Customer acknowledges that it subscribes to receive various information services in accordance with the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999), as amended (the "VFCRA") and the Federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. Seq., as amended (the "FCRA") and its other state law counterparts. In connection with Customer's continued use of RT services in relation to Vermont consumers, Customer hereby certifies as follows: Vermont Certification. Customer certifies that it will comply with applicable provisions under Vermont law. In particular, Customer certifies that it will order information services relating to Vermont residents that are credit reports as defined by the Vermont Fair Credit Reporting Act ("VFCRA"), only after Customer has received prior consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Customer further certifies that the below copy of Section 2480e of the Vermont Fair Credit Reporting Statute was received.

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:

i. the report is obtained in response to the order of a court having jurisdiction to issue such an order; or

ii. 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:

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

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