



CUSTOMER APPLICATION

Company Information

Company Name: _____
Address (no PO Box): _____
City: _____ State: _____ Zip: _____
Address Type: Commercial Residential Time at Address: ___ Yr ___ Mo
Phone: _____ Fax: _____
Website: _____
Nature of Business (bank, mortgage broker, credit union, etc): _____
Date Established: _____ Number of Employees: _____
Federal Employer ID Number (EIN): _____
Ownership: Sole Owner Partnership Corporation LLC Non-Profit
Customer Base: Local Regional National Est. Monthly Volume: _____ Reports

Primary Contact

Name: _____
Title: _____
Address _____
City: _____ State: _____ Zip: _____
Phone: _____ Fax: _____
Email: _____

References

Bank Name _____
Account Number _____ Date Opened _____
Address _____ City _____ State _____ Zip _____
Phone _____ Contact Person _____
Creditor Name _____
Account Number _____ Date Opened _____
Address _____ City _____ State _____ Zip _____
Phone _____ Contact Person _____

Guarantor

Guaranteed By _____ SSN _____ - _____ - _____
Home Address _____
City _____ State _____ Zip _____
Phone _____ Fax _____ Email _____
Signature of Guarantor _____



SERVICE AGREEMENT

This Service Agreement (“Agreement”) is made on this ___ day of _____, 20__ (“Effective Date”) entered into by and between Old Republic Credit Services, a California corporation with an address located at 65 E. Wacker Place, Suite 1405, Chicago, IL 60601 and _____ a _____ corporation located at _____ (“Applicant”).

Applicant requests the Services upon the basis outlined below, and if accepted by Old Republic Credit Services as a customer, agrees that the following shall constitute an enforceable contract between the Applicant and Old Republic Credit Services.

1. SERVICES.

- (a) Old Republic Credit Services is a consumer reporting agency (“CRA”) that is in the business of selling “Consumer Reports” (as that term is defined in the Fair Credit Reporting Act (“FCRA”)) and other products and services (collectively, the “Services”). These Services include merged reports that include information from one or more of the national credit information repositories, Equifax, Trans Union, and Experian (“Repositories”).
- (b) Old Republic Credit Services agrees to provide Applicant with Services, including “Consumer Reports”, on individuals, firms or corporations, including but not limited to identifying information, credit history, employment and public record information, in file, such information being furnished at the special request of Applicant.

2. PERMISSIBLE PURPOSE.

- (a) Applicant warrants that it is a _____ (type of business) and has a permissible purpose for obtaining Consumer Reports as defined by Section 604 of the Federal Fair Credit Reporting Act (15 USC 1681b), hereinafter called the “FCRA.” Applicant certifies their permissible purpose as (please check each box that applies):
- (i) In connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of the consumer; or
- (ii) 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
- (iii) In connection with a tenant screen application involving the consumer; or
- (iv) In accordance with the written instructions of the consumer; or
- (v) For a legitimate business need in connection with a business transaction that is initiated by the consumer; or
- (vi) As a potential investor, servicer or current insurer in connection with a valuation of, or assessment of, the credit or prepayment risks.



(b) Applicant will use the Services for the specific purpose of _____.

(c) Applicant acknowledges that it will use 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 Applicant's continued use of Services in relation to Vermont consumers, Applicant hereby certifies that it will comply with applicable provisions under Vermont law. In particular, Applicant certifies that it will order information Services relating to Vermont residents, that are credit reports as defined by the VFCRA, only after Applicant has received prior consumer consent in accordance with VFCRA § 2480e and applicable Vermont Rules. Applicant further certifies that the attached copy of § 2480e (**Exhibit A**) of the Vermont Fair Credit Reporting Statute was received from Old Republic Credit Services.

(d) If applicant does any business in California, Applicant certifies that Applicant is not a retail seller as defined in Section 1892.3 of the California Civil Code.

3. ACCESS SECURITY AND SITE INSPECTION. Applicant will maintain internal procedures to minimize the risk of unauthorized disclosure of the Services including following the internal controls outlined in **Exhibit B**. A third party physical inspection of each of Applicant's unique business locations that will be receiving the Services must be completed prior to each such unique location's receiving the Services. The costs of these inspections shall be borne by Applicant.

4. TERMS OF SERVICE.

(a) Applicant certifies that it will request the Services pursuant to procedures prescribed by Old Republic Credit Services only for the permissible purpose(s) certified above, and will use the Services obtained for no other purpose, and that Applicant will obtain the authorization of the consumer prior to obtaining a Consumer Report on the consumer. Applicant will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.

(b) The Services will be requested only for applicant's exclusive use. **APPLICANT WILL NOT RESELL THE SERVICES TO ANY THIRD PARTY.**

(c) Applicant shall use each of the Services 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 Applicant may, but is not required to, disclose a Consumer Report to the subject of the report in connection with an adverse action based on the report.

(d) Applicant shall not disclose to any third party other than the subject of the report, any credit scores and associated reason codes provided under this Agreement, unless clearly required by law. Reports and credit scores may be disclosed to properly credentialed and contracted third-parties for certified FCRA permissible purposes of secondary use within the course of the same transaction. Applicant agrees to abide by the Secondary Use policy outlined in **Exhibit C**.

(e) Applicant understands that the Repositories may periodically audit Applicant directly or via Old Republic Credit Services regarding compliance with the FCRA. Audits will require Applicant to provide documentation as to permissible use and authorization of particular consumer reports, including, but not limited to, a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract. Applicant will provide full cooperation during audits and will be responsible for assuring full cooperation of its employees. Violations discovered in the course of an audit are subject to immediate action including, but not limited to, termination of service agreement, legal action, and referral to federal or state regulatory authorities.



5. FAIR CREDIT REPORTING ACT.

- (a) Applicant will become intimately familiar and comply with all the provisions of the Fair Credit Reporting Act (“FCRA”) and all other applicable State and Federal laws applicable to consumer credit information.
- (b) Both parties represent that in accordance the FCRA and the FTC Final Rule, 16 CFR, Part 682 that they have implemented reasonable measures to protect against unauthorized access or use of the information in connection with the disposal of consumer information as that term is defined in the FTC Final Rule.
- (c) 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, OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.
- (d) 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.”

6. CONFIDENTIAL INFORMATION.

- (a) Each party agrees that information concerning the other party's business (including that of all corporate affiliates and subcontractors) is "Confidential Information" and proprietary to that party and shall be maintained in confidence and not disclosed, used or duplicated, except as described in this section. Confidential Information may include, without limitation, lists of, or other information relating to and identified with customers, former or prospective customers or applicants, business volumes or usage, financial information, pricing information, information related to mergers or acquisitions, security procedures, information concerning business plans or business strategy, patent, copyright, trade secret, and other proprietary information, software and software documentation, data, inventions, know-how, processes, information related to the party's current, future, and proposed products and services, and the subject matter of this Agreement. Confidential Information does not include information that is generally known or available to the public or that is not treated as confidential by the disclosing party, provided, however, that this exception shall not apply to any publicly available information to the extent that the disclosure or sharing of the information by one or both parties is subject to any limitation, restriction, consent, or notification requirement under any applicable federal or state information privacy law or regulation.
- (b) Both parties agree to protect Confidential Information and may only disclose such information to its employees having a need to know and who are otherwise bound by confidentiality obligations at least as restrictive as those contained in this Agreement. Both parties shall use the same care to prevent disclosure of Confidential Information as it uses with respect to its own Confidential Information. The receiving party may use Confidential Information only in connection with performance under this Agreement. Except as described in this Agreement, the receiving party shall not copy Confidential Information or disclose Confidential Information to persons who do not need Confidential Information in order to perform under this Agreement.

7. NONPUBLIC PERSONAL INFORMATION. Both parties shall comply with Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (“GLB Act”) and the implementing regulations and will not use or disclose any nonpublic personal information (“Personal Information”) furnished to the other except in accordance with the GLB Act or the FCRA. Both parties represent that they have established and maintain appropriate measures designed to meet the objectives outlined in the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth in 501 and 505 of the GLB Act (15 U.S.C. § 6801 and § 6805). The parties have in place programs designed to ensure the security and confidentiality of the Personal Information, to protect



against any anticipated threats or hazards to the security or integrity of the Personal Information and to protect against unauthorized access to or use of such Personal Information.

8. UNLAWFUL USE. Applicant specifically and unconditionally agrees to fully indemnify and reimburse ORCS for all costs, liabilities or other losses arising from the improper, unauthorized, or otherwise unlawful use of any usernames, passwords or access codes associated with Applicant's ORCS network account. In particular, Applicant specifically and unconditionally agrees to reimburse and indemnify ORCS for ALL COSTS ORCS incurs as a result of the unauthorized, illegal, fraudulent or otherwise improper use of Applicant's passwords or security credentials to gain access to consumer data held by any of the three national credit bureaus, including TransUnion, Experian and Equifax, or any other sensitive consumer data. In the event of such unauthorized or improper use of Applicant's passwords to gain access to consumer data, ORCS is required by law to initiate a number of security measures to protect affected consumers, including but not limited to, purchase of fraud monitoring products for such consumers, regulatory, administrative and attorney reviews of the incident and compliance measures, as well as consumer notification, and notification to and cooperation with appropriate federal, state and local law enforcement. ANY AND ALL COSTS ASSOCIATED WITH SUCH MEASURES, INCURRED BY ORCS, SHALL BE BORN BY APPLICANT WITHOUT LIMITATION. In the event of such an improper or unauthorized access event, ORCS will provide a detailed accounting of ORCS incurred costs to the applicant with a demand for payment. Applicant hereby agrees that in such an event it shall reimburse ORCS within 30 calendar days of the demand and accounting. In addition, following the improper or unauthorized access, Applicant's access to the ORCS network may be suspended for a reasonable time, or indefinitely, pending the outcome of any investigation into the incident by law enforcement or any affected private party. In no event shall ORCS bear any liability for losses incurred by applicant during such a suspension period, resulting from said suspension in any way.
9. TERM AND TERMINATION. This agreement shall remain in force and effect for one year and thereafter, from year to year, on the same basis as set forth herein until written notice of cancellation shall be given by either party at least 10 days prior to the end of the then current monthly period. It is further agreed, however, that if the Applicant is delinquent in the payment of the monthly charges, or is guilty of violating the terms of this contract, or if there is a material change in existing legal or regulatory requirements which adversely affects this Agreement, Old Republic Credit Services may, at its election, discontinue providing service to the Applicant and/or cancel this contract immediately by written notice to the Applicant.
10. PRICING AND PAYMENT. Pricing and payment terms are described in a separate Pricing Confirmation Letter. Old Republic Credit Services shall have the right to recover expenses, including collection costs and reasonable attorney's fees incurred in collecting overdue amounts. The undersigned Guarantor personally guarantees any and all charges incurred in connection with this agreement and account. The undersigned Guarantor authorizes Old Republic Credit Services to obtain, from time to time, consumer credit and other public record reports on Guarantor in connection with any extension of credit to, or review or collection of the account of Applicant and/or Guarantor.
11. PROTECTED MARKS. Applicant shall not use the trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of Old Republic Credit Services, Experian, Equifax, Trans Union, or Fair, Isaac, other third party suppliers of Old Republic Credit Services, or any of the affiliates of the above listed companies.
12. AMENDMENTS. Old Republic Credit Services reserves the right to revise the terms, conditions, or pricing under this Agreement in order to meet any requirement imposed by federal, state or local law, rule or regulation, or to address matters concerning privacy and confidentiality. If at any time during the duration of this business relationship the undersigned party becomes no longer affiliated with Applicant, Old Republic Credit Services reserves the right to suspend the account immediately until a new Agreement is signed by a valid representative of the Applicant.



13. ENTIRE AGREEMENT. This Agreement constitutes the entire agreement between the parties and supersedes all prior oral or written agreements or representations. No modification of this Agreement (including any additional or different terms) shall be binding unless agreed to in writing.
14. ASSIGNMENT. This Agreement is not assignable to any other party regardless of circumstances, including change of ownership or control of business without prior consent of Old Republic Credit Services. Applicant must notify Old Republic Credit Services of any changes in ownership, business name or business locations. These changes may require additional documentation and assurances to Old Republic Credit Services.
15. MONITORING. Old Republic Credit Services will monitor Applicant on an ongoing basis to assure the continued compliance with the requirements of the Service Agreement.
16. WAIVER. No course of dealing or failure by Old Republic Credit Services to strictly enforce any term, right, or condition of this Agreement shall be construed as a waiver of such term, right, or condition.
17. GOVERNING LAW: JURISDICTION. This Agreement shall be governed by and construed in accordance with the laws of the state of California, without reference to the principles of conflict of laws of such state.
18. FORCE MAJEURE. Neither party to this Agreement shall be considered to be in default of its obligation under this Agreement to the extent that failure to perform any such obligation arises from causes beyond the control and without the fault or negligence of the affected party. Such acts shall include, but not be limited to, acts of God, riots, acts of war, epidemics, failure of suppliers to perform, governmental regulations, power failures, earthquakes, and other disasters.
19. SEVERABILITY. If any provision of this Agreement is or becomes void or unenforceable by force or operation of law, the other provisions shall remain valid and enforceable.
20. RELEASE WITH RESPECT TO CREDIT INFORMATION. Applicant acknowledges that Old Republic Credit Services' suppliers maintain databases updated on a periodic basis and that Old Republic Credit Services' suppliers do not undertake a separate investigation for each inquiry or request for Services made by Applicant. Applicant acknowledges that the prices charged for the Services are based upon the expectation: (a) that the risk of any loss or injury that may be incurred by use of the Services will be borne by Applicant and not by Old Republic Credit Services or its suppliers; and (b) that neither Old Republic Credit Services nor any of its suppliers are an insurer or guarantor of the accuracy or reliability of the Services. NEITHER OLD REPUBLIC CREDIT SERVICES NOR ITS SUPPLIERS GUARANTEES OR WARRANTS THE ACCURACY, TIMELINESS, COMPLETENESS, CURRENTNESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE SERVICES, INFORMATION IN THE SERVICES OR THE MEDIA ON OR THROUGH WHICH THE SERVICES ARE PROVIDED. NEITHER OLD REPUBLIC CREDIT SERVICES NOR ITS SUPPLIERS SHALL BE LIABLE TO CLIENT FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY THE ACTS OR OMISSIONS OF OLD REPUBLIC CREDIT SERVICES AND ITS SUPPLIERS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE SERVICES OR INFORMATION THEREIN.
21. INDEMNIFICATION. Applicant releases, indemnifies, defends and holds Old Republic Credit Services, its suppliers, and their respective officers, directors, employees, contractors, agents, subscribers or affiliates, harmless from and against any and all liabilities, damages, losses, claims, costs and expenses, including reasonable attorneys' fees and costs, which may be asserted against or incurred by any indemnified person, arising out of, resulting from or threatening to result from: (a) the access to, or the use, disclosure, sale or transfer of, or the reliance on, the services provided by Old Republic Credit Services (the "Services") by Applicant; (b) any inaccuracies contained in any credit or other information; (c) violations of the FCRA or other applicable state and federal laws and regulations due to the acts or omissions of Applicant; (d) any breach or



nonperformance by Applicant of any obligations to be performed by Applicant under this Agreement (including without limitation any improper or unauthorized access to or disclosure of information obtained via any Applicant Account Code/Password or system); (e) Applicant's negligence, malfeasance, or tortious conduct; Applicant acknowledges that the Services are furnished in reliance upon Applicant's indemnities and covenants under this Agreement. Such indemnities and covenants shall survive any termination or expiration of this Agreement.

22. DISCLAIMER OF WARRANTIES.

- (a) NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL OLD REPUBLIC CREDIT SERVICES OR ANY OF ITS SUPPLIERS HAVE ANY OBLIGATION OR LIABILITY TO APPLICANT'S CLIENTS, CUSTOMERS OR ANY OTHER THIRD PARTY HEREUNDER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, WARRANTY, OR OTHERWISE: (a) FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY A THIRD PARTY, REGARDLESS OF HOW SUCH DAMAGES, WHETHER FORESEEABLE OR NOT AND HOWEVER CAUSED, EVEN IF OLD REPUBLIC CREDIT SERVICES OR ITS SUPPLIERS ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; OR (b) FOR ANY PUNITIVE OR EXEMPLARY DAMAGES.
- (b) Applicant acknowledges that any score generated by a proprietary model and furnished to Applicant is the proprietary information of the Old Republic Credit Services supplier that generated such score. Applicant shall not attempt, in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by any Old Republic Credit Services supplier in generating a score or using such supplier's model. National repository suppliers each offer scores developed in conjunction with models developed by Fair Isaac Companies or others (each a "Risk Model") and have made limited warranties with respect to scores, subject to certain limitations, as follows: (a) that the applicable Risk Model is intended to be empirically derived and demonstrably and statistically sound; (b) that to the extent the population to which the Risk Model is applied is similar to the population sample on which the Risk Model was developed, a FICO score may be relied upon to rank consumers in order of the risk of unsatisfactory payments such consumers might present to Applicant; (c) that so long as the repository provides a Risk Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act (15 USC § 1692 *et seq.*); (d) THAT THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES GIVEN WITH RESPECT TO A RISK MODEL OR SCORE AND THAT SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, THAT MIGHT HAVE GIVEN WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE; and (e) that Applicant's rights under the foregoing warranties are expressly conditioned upon Applicant's periodic revalidation for the applicable Risk Model in compliance with the requirements of Regulation B as amended from time to time. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF OLD REPUBLIC CREDIT SERVICES OR ANY SCORE SUPPLIER TO CLIENT EXCEED THE LESSER OF THE FEES PAID (1) BY CLIENT TO OLD REPUBLIC CREDIT SERVICES OR (2) BY OLD REPUBLIC CREDIT SERVICES TO THE SCORE SUPPLIER, FOR THE SCORES SOLD TO CLIENT DURING THE TWELVE MONTH PERIOD IMMEDIATELY PRECEDING THE CLIENT'S CLAIM.



**OLD REPUBLIC
CREDIT SERVICES**

65 E. Wacker Place Suite 1405, Chicago, IL 60601 | Phone: 888.895.5145 | Fax: 888.895.5146

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the Effective Date.

_____ Applicant (Company Name)	_____ OLD REPUBLIC CREDIT SERVICES Consumer Reporting Agency
_____ Authorized Signature	_____ Authorized Signature
_____ Date	_____ Date
_____ Printed Name	_____ Printed Name
_____ Title	_____ Title

EXHIBIT A

Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999)

§ 2480e. Consumer consent

- (a) A person shall not obtain the credit report of a consumer unless:
 - (1) the report is obtained in response to the order of a court having jurisdiction to issue such an order; or
 - (2) the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer.
- (b) Credit reporting agencies shall adopt reasonable procedures to assure maximum possible compliance with subsection (a) of this section.
- (c) Nothing in this section shall be construed to affect:
 - (1) the ability of a person who has secured the consent of the consumer pursuant to subdivision (a)(2) of this section to include in his or her request to the consumer permission to also obtain credit reports, in connection with the same transaction or extension of credit, for the purpose of reviewing the account, increasing the credit line on the account, for the purpose of taking collection action on the account, or for other legitimate purposes associated with the account; and
 - (2) the use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade Commission.

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

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

EXHIBIT B

Access Security Requirements

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. Old Republic Credit Services reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security.

In accessing consumer credit services from Old Republic Credit Services, you agree to follow these measures:

1. Implement Strong Access Control Measures

- 1.1 Do not provide your Old Republic Credit Services system usernames or passwords to anyone. No one from Old Republic Credit Services will ever contact you and request username or password.
- 1.2 Proprietary or third party system access software must have username(s) and password(s) hidden or embedded. Only supervisory personnel should know Usernames and passwords.
- 1.3 You must request your password be changed immediately when:
 - any system access software is replaced by system access software or is no longer used;
 - the hardware on which the software resides is upgraded, changed or disposed of
- 1.4 Protect Old Republic Credit Services usernames(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your username(s) and password(s).
- 1.5 Create a separate, unique username for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that usernames are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 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
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 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 information are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.
- 1.13 Ensure that you and your employees do not access your 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.
- 1.14 Implement a process to terminate access rights immediately for users who access credit reporting agency 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.
- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

2. Maintain a Vulnerability Management Program

- 2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- 2.2 Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, 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 Computer Virus detection/scanning product on all computers, systems and networks.
 - 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.
 - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
 - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
 - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
 - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
 - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

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 All credit reporting agency data is classified as Confidential and must be secured to this requirement 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 credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

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 Safeguard Rule.
- 4.2 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.
- 4.3 The FACTA Disposal Rules requires that you 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.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

5. Build and Maintain a Secure Network

- 5.1 Protect Internet connections 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 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

6. Regularly Monitor and Test Networks

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 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.

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, 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 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.”

EXHIBIT C

Secondary Use Policy

1. SECONDARY USE DEFINED. A Secondary Use of a credit report occurs when a previously ordered report is provided to any Qualified Secondary User other than the End User that originally ordered the credit report, in connection with the same transaction for a permissible purpose.

Secondary Use occurs when any or all of the consumer credit data contained in the original report is provided to the Qualified Secondary User in any form: electronic, paper or otherwise. As the original requestor of the consumer credit data, Old Republic Credit Services customers are defined as the original End User for the purpose of Secondary Use.

2. QUALIFIED SECONDARY USERS. A Qualified Secondary User is a lender or other third party that has been properly credentialed as having a permissible purpose under the Fair Credit Reporting Act (FCRA) to access consumer credit data.

3. SECONDARY USE PURPOSE. The purpose of Secondary Use reporting is to provide greater transparency to the consumer as to which entities are viewing consumer credit data in the mortgage loan application and underwriting process. Additionally, Secondary Use reporting ensures that consumer credit data is only accessed in accordance with FCRA guidelines.

4. SECONDARY USE INQUIRY POSTING. The three national credit repositories, TransUnion, Equifax and Experian, mandate that all Secondary Uses be reported for the purposes of posting to the consumers credit file in accordance with the FCRA. The repositories post Secondary Uses to consumers' credit files as "soft" inquiries that do not impact the consumers' credit scores and will only be displayed on consumer disclosure reports. The Secondary Use notification sent to the repositories must include the full name of the Qualified Secondary User for posting to the consumer's credit file. The repositories charge for each Secondary Use Inquiry posted.

5. SECONDARY USE FEES. TransUnion, Equifax, and Experian each charge a Secondary Use posting fee for every secondary inquiry that is reported on a consumer's file. Old Republic Credit Services will impose a Secondary Use fee on our customers for each Secondary Use transaction.

6. OLD REPUBLIC CREDIT SERVICES RESPONSIBILITIES. As the original reseller of the consumer credit data, Old Republic Credit Services is responsible for reporting all Secondary Use transactions to TransUnion, Equifax, and Experian for reporting to consumers' credit files. Old Republic Credit Services currently has agreements with the Government Sponsored Entities (Fannie Mae and Freddie Mac) as well as other major lenders to record Secondary Use transactions from these qualified entities.

7. APPLICANT RESPONSIBILITIES. As the original End User of consumer credit reports, the Applicant must abide by the following:

(a) Applicant must ensure that all Secondary Uses of credit reports to Qualified Secondary Users are reported to Old Republic Credit Services for accurate posting to the repositories.

(b) Applicant is prohibited from distributing consumer credit reports, in whole or in part, by any means, to entities or individuals that are not Qualified Secondary Users.

(c) Applicant is prohibited from distributing consumer credit reports to any secondary user that does not have permissible purpose under the FCRA to access consumer credit data.

(d) Applicant is prohibited from distributing consumer credit reports to any secondary user that is not in connection with the transaction the report was originated for.