PLEASE READ THESE INSTRUCTIONS CAREFULLY BEFORE YOU BEGIN THE APPLICATION

An approved membership with Innovative Credit Solutions will give you access to protected consumer information from the Experian bureau. Please read, fill out and sign the application completely. Your signature acknowledges you have read and will comply with the provisions within these documents. Please fax the completed application (pages 1 through 15) and a copy of your business license to 888-571-7222.

- All pages must be signed and completed (no exceptions).
  - Page 1 – Application Form – you may enter the information electronically or a hand-written copy is acceptable. Please make sure the credit card information is correct and the page is signed.
  - Pages 2 & 3 – Broker Subscriber Agreement – top of page 2 - print the name of your company in the blank; bottom of page 3 - print your name & company name; sign & date
  - Page 4 – FCRA Requirements – print your company name (End User), your name and title; sign & date
  - Pages 5 to 10 – Access Security Requirements – page 9 - print your company name and your name; sign & date
  - Pages 11 & 12 – Scoring Services Agreement – print the date and your company name at the top of page 11; print your company name, your name, sign & date page 12
  - Page 13 – Employment Use Certification – complete and sign if reports will be pulled for employment purposes
  - Pages 14 & 15 – California & Vermont Provisions - print your name, title, company name; sign & date – these pages must be signed whether or not you are doing business in these states
  - Pages 16 & 17 – Fair Credit Reporting Act Summary of Rights – You do not need to return these pages

- You must provide the physical address where the consumer reports will be accessed. This is the address we need for the inspection. If there is a different billing contact and address, please provide.
- We must have a copy of your business license or a copy of the document that your state requires to operate a business. A copy of the current White or Yellow Pages ad for your business may be sufficient. -**OR-**
- If this application is for **Tenant Screening** by an individual who owns or manages property, then send the following:
  a. A copy of three signed tenant applications
  b. A list of the properties - description and address
- We will need a telephone number and contact person that can be reached during the day. An e-mail address and fax number is also needed.
- If you do not have a shredder, please purchase one prior to the inspection, consumer information must be shredded when you no longer need it.
- The office where the consumer reports will be accessed must have a locking door or locking file cabinet.
- If your business is operated from a private residence, the office must be in a separate room with a locking door. There can be no evidence of any other activity in that room other than the business.
- NCCI, Trendsource, and CRM Inspections are the companies we use for the onsite inspection of your business. A representative from one of those companies will contact you to set up an appointment for the inspection.

If you have any questions, please call us at 800-345-2746 or e-mail your questions to info@icscredit.com. We also offer criminal background and driver record checks to assist you in making a well-informed decision about extending credit or offering employment.

INNOVATIVE CREDIT SOLUTIONS, INC.

Phone: 1-800-345-2746
Fax: 1-888-571-7222
info@icscredit.com

P O Box 1440
Lexington, SC 29071
www.icscredit.com

APPLICATION FOR SERVICE

COMPLETE ALL INFORMATION AND SIGN APPLICATION
INCLUDE COPY OF BUSINESS LICENSE WITH APPLICATION

BUSINESS INFORMATION

Name of Firm				Federal Tax ID#	
Other business name(s) or dba				Web Address	
Phone:	Fax:		E-mail:		
Physical Address (No PO Box numbers)					
City:			State:	ZIP Code:	
Business Established:	Month	Year	How long at current address:	Years	Months
Does your business operate from a residence ☐ YES ☐ NO			Number of Employees:		
Contact Name:			Title:		
Phone:	Fax:		E-mail:		
Company name as listed with Directory Assistance:					
Nature of your Business (be specific):					
Services offered or products sold:					
Permissible Purpose/Appropriate Use: ☐Extending Credit ☐Employment Purposes ☐Tenant Screening ☐Other Describe the specific purpose for which credit information will be used. ***This field must be completed***					
I ☐ will ☐ will not be requesting consumer reports in ☐ California ☐ Vermont					
Business Hours:	Business Days:				

BILLING INFORMATION

Billing Contact:	Phone:	E-mail:

Cost to Activate Account: $75.00 Annual Fee & $75.00 Set-Up Fee (onsite inspection) = $150.00

☐ Option 1: $15.00 per consumer credit report
☐ Option 2: $7.50 per consumer credit report with $20.00 Monthly Minimum

CREDIT CARD INFORMATION ☐ American Express ☐ Visa ☐ MasterCard ☐ Discover

Credit Card #:	Exp Date	CVV # (digits on back of card)
Name on Card:		

Billing Address on Card:	City	State	Zip

Federal regulation requires that ICS, Inc. conduct an onsite property observation of your company. In most cases, this must be conducted prior to your account being established. Please note that ICS, Inc. contracts with a vendor to conduct these property observations and that vendor will be contacting you on behalf of ICS, Inc. to schedule an appointment. (The vendor usually contacts you within three days of receipt of application.)

SIGNATURE & AGREEMENT

I certify that I will use the Experian, Equifax, TransUnion background information for no other purpose other than what is stated in the Permissible Purpose/Appropriate Use section on this application and for the type of business listed on this application. **I will not resell the report to any third party.** I understand that if my system is used improperly by company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated. By signing below I authorize Innovative Credit Solutions, Inc. to charge the above listed credit card for all services provided. I certify that the above information is accurate. By signing, I warrant that I have the authority to sign on behalf of the company. I acknowledge that an onsite inspection will be required for new customers. A copy of the Company business license is included with this application.

Principal's Name (please print)	Title or Position:
Principal's Signature (required):	Date:

INNOVATIVE CREDIT SOLUTIONS, INC.

BROKER SUBSCRIBER AGREEMENT

The undersigned (hereinafter referred to as the Subscriber) _____ desiring to receive various information services as available through Innovative Credit Solutions, Inc., (hereinafter referred to as ICS), a reseller of consumer credit reports and other information agrees that all information obtained will be subject to the following conditions:

EMPLOYMENT PURPOSES: Information obtained through ICS will be requested only for Subscriber's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted by law. Only designated representatives of Subscriber will request information on Subscriber's employees, and employees will be forbidden to obtain reports on themselves, associates or any other persons except in the exercise of their official duties. Subscriber agrees that each time a request is made for information on a credit report for employment purposes, Subscriber will comply with §604 of the FCRA, namely:

1) The consumer has been given a clear and conspicuous written notice, in evidence (in a document that consists solely of the disclosure), that a consumer report may be requested for employment purposes.
2) The consumer has authorized the Subscriber, in writing to procure the report.
3) The information in the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.
4) Before taking adverse action, in whole or part on the report, Subscriber will provide the consumer a copy of the report and a description of the consumer's rights under the FCRA. A copy of which is attached hereto ("Summary of the Consumers Rights").

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

Recognizing that information obtained through ICS is secured by and through fallible human sources and that, for the fee charged, ICS, Equifax and Experian cannot be an insurer of the accuracy of the information obtained. Subscriber understands that the accuracy of any information received by a Subscriber is not guaranteed by ICS, Equifax or Experian and Subscriber releases ICS, Equifax, Experian and its affiliate companies, affiliated credit bureaus, agents, employees, and independent contractors or indirectly from the information obtained.

CREDIT SCORES: If a score is obtained, Subscriber agrees that Fair Issac, ICS, Equifax, Experian, their Officers, directors, employees, agents, sister or affiliated companies or any third party contractors or suppliers are not responsible for any loss of profits, special, indirect, consequential or exemplary damages, costs or expenses in connection with the use or performance of scores even if advised of the possibilities of such damages. Subscriber understands that ICS, Equifax or Experian do not guarantee the predictive value of a score. Subscriber releases ICS, Equifax, Fair Isaac, Experian, their officers, employees, agents, sister of affiliated companies or any third party contractors or suppliers from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by Subscriber resulting from the use of a score or any failure of score to accurately predict the credit worthiness of Subscriber's applicants and customers in connection with Subscriber's actions in regard to its applicants and customers.

Written notice by either party to the other will terminate this Agreement effective ten days after the date of that notice, but the obligations and agreements set forth in the second, third, and fourth paragraphs above will remain in force.

Subscriber certifies that it will order consumer reports, as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq ("FCRA") only when Subscriber intends to use that consumer report information: (a) in accordance with the FCRA and all state law counterparts; and (b) for one of the following permissible purposes:

a) 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 connection of an account of, the consumer, or
b) For employment purposes; provided Subscriber follows guidelines of Paragraph 2 above and will comply with §604 of the FCRA, or
c) In connection with the underwriting of insurance involving the consumer, or
d) In connection with the legitimate business need for the information in connection with a business transaction initiated by the consumer or to review an account to determine whether the consumer continues to meet the terms of the account; and the Applicant agrees to identify to ICS each request at the time such report is ordered, and to certify the legitimate business need for such report; or
e) As a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with an existing credit obligation.

Subscriber will use each consumer report ordered under this Agreement for one of the foregoing purposes.

Subscriber agrees that any person designated as an authorized user in obtaining consumer reports is aware of the obligations of the Subscriber and its authorized users under this agreement including the FCRA and other obligations with respect to the access and use of consumer reports. Subscriber will (a) ensure that all consumer information be kept in a secure area and only accessible by authorized users; (b) ensure that only the authorized users can order the consumer reports; and, (c) ensure that the authorized user does not order credit reports for personal reasons or provide them to any third party.

Subscriber will maintain copies of all written authorizations for a minimum of three (3) years from the date of inquiry. When consumer reports are not longer needed they are to be shredded. Subscriber agrees that it shall use consumer reports only for a one-time use, and to hold the report in strict confidence, and not to disclose it to third parties. Subscriber will also inform authorized users and other employees with a need to know that unauthorized access to consumer reports may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment.

Subscribers may discuss information obtained through ICS with the consumer in the event Subscriber declines or takes adverse action regarding the consumer. ICS, Equifax and Experian shall not be liable in any manner whatsoever for any loss or injury to applicant resulting from the obtaining or furnishing of such information and shall not be deemed to have guaranteed the accuracy of such information, such information being based, however, upon reports obtained from sources considered to be reliable.

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 Experian services contain information from the DMF, Experian would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within the Experian 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 Experian 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 the Experian services.

By signing below Subscriber acknowledges that Subscriber has read agreement and all Exhibits including but not limited to California Retail Seller Compliance and the Vermont Fair Credit Statute, 9 V.S.A. §2480e (1999) and understands and agrees to all conditions of this agreement. Subscriber also agrees that if reports are requested for Employment Purposes, Subscriber will comply with Paragraph 2 above and guidelines outlined in §604 of the FCRA. To view the FCRA in its entirety go to http://www.ftc.gov/os/statutes/031224fcra.pdf.

Subscriber also understands that it is solely the responsibility of the Subscriber to know the conditions outlined in the FCRA and other state and federal laws concerning the use of consumer reports and information. By signing this agreement, subscriber acknowledges they have read and understand the "FCRA Requirements" notice and "Access Security Requirements" and will take all reasonable measures to enforce them within their facility. Subscriber further agrees they will not resell the report to any third party.

The undersigned is a duly authorized representative of Subscriber with all powers to execute this Agreement.

SIGNATURE_____

DATE_____

PRINT NAME_____ TITLE _____

FCRA Requirements

Federal Fair Credit Reporting Act (as amended by the
Consumer Credit Reporting Reform Act of 1996)

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. A copy of the FCRA is available on the FAQ tab of our website: www.icscredit.com. We suggest that you and your employees become familiar with the following sections 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.

As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as in investment, partnership, etc. It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

We strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

In addition to the Federal Fair Credit Reporting Act, other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate.

We support consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information.

End User _____

SIGNATURE_____ DATE _____

PRINT NAME_____

TITLE _____

Access Security Requirements for FCRA and GLB 5A Data

(rev 11/2014)

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

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

1. Implement Strong Access Control Measures

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

1.2 If using third party or proprietary system to access Innovative Credit Solutions' 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 Innovative Credit Solutions data/systems.

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

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

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

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

1.7 Develop strong passwords that are:

- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

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

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

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

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

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

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

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

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

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

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

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

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

2. Maintain a Vulnerability Management Program

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

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

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. 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.

3. Protect Data
3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).
3.2 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.
3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
3.4 Encrypt all Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.
3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.
3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.
3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.
3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.
3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).
4. Maintain an Information Security Policy
Implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by Reseller; and that such safeguards shall include the elements set forth in 16 C.F.R. section 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Reseller, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer
4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.
4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.
4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe Experian data may have been compromised, immediately notify Innovative Credit Solutions within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*
4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.
4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*
5. Build and Maintain a Secure Network
5.1 Protect Internet 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 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.
5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.
5.7 When using service providers (e.g. software providers) to access Innovative Credit Solutions systems, access to third party tools/services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)
6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data; establish a process for linking all access to such systems and applications. Ensure 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 Innovative Credit Solutions systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

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

7. **Mobile and Cloud Technology**

7.1 Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian in writing; additional security requirements will apply.
7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.
7.3 Mobile 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.
7.4 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.
7.5 Mobile 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 Experian data to be exchanged between secured and non-secured applications on the mobile device.
7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Experian data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.
7.7 When using cloud providers to access, transmit, store, or process Experian data ensure that:

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

8. **General**

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

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

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

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

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.
8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.
8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.
8.5 Reasonable access to audit trail reports of systems utilized to access Innovative Credit Solutions systems shall be made available to Innovative Credit Solutions upon request, for example during breach investigation or while performing audits
8.6 Data requests from Company to Innovative Credit Solutions must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.
8.7 Company shall report actual security violations or incidents that impact Experian to Innovative Credit Solutions within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Innovative Credit Solutions 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 800-345-2746, Email notification will be sent to info@icscredit.com.
8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Innovative Credit Solutions services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.
8.9 Company understands that its use of Innovative Credit Solutions networking and computing resources may be monitored and audited by Innovative Credit Solutions, without further notice.
8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access Innovative Credit Solutions services or data are secure and in compliance with its membership agreement.
8.11 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by Innovative Credit Solutions.

Record Retention: The Federal Equal Credit Opportunity Act *states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Experian requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract. "Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable* for a civil penalty of not more than $3,500 per violation."

Internet Delivery Security Requirements
In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Innovative Credit Solutions provided services via Internet ("Internet Access").
General requirements:
1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Innovative Credit Solutions on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Innovative Credit Solutions provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Innovative Credit Solutions product based upon the legitimate business needs of each employee. Innovative Credit Solutions shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Innovative Credit Solutions. 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). Innovative Credit Solutions' approval of requests for (Internet) access may be granted or withheld in its sole discretion. Innovative Credit Solutions 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 Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. *Note: Partially completed forms and verbal requests will not be accepted.*

4. An officer of the Company agrees to notify Innovative Credit Solutions 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.

Roles and Responsibilities

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

Designate

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

Subscriber: _____
(please print)

Signature: _____

Print Name: _____

Date: _____

Glossary Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Subscriber Code	Your seven digit Experian account number.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.
ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided

EXPERIAN CREDIT SCORING SERVICES AGREEMENT

This Credit Scoring Services Agreement, ("Agreement"), dated _____ between _____ ("End User") and Innovative Credit Solutions, Inc. ("Provider")

WHEREAS, Provider is an authorized reseller of Experian Information Solutions, Inc ("Experian"); and

WHEREAS, Experian and Fair Isaac Corporation ("Fair Isaac") offers the "Experian/Fair Isaac Model") consisting of the application of a risk model developed by Experian and Fair Isaac which employs a proprietary algorithm and which, when applied to credit information relating to individuals with whom the End User contemplates entering a credit relationship will result in a numerical score (the "Score" and collectively, "Scores"); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

NOW, THEREFORE, For good and valuable consideration and intending to be legally bound, End User and Provider hereby agree as follows:

1. General Provisions

A. **Subject of Agreement**. The subject of this Agreement is End User's purchase of Scores produced from the Experian/Fair Isaac Model from Provider.

B. **Application**. This Agreement applies to all uses of the Experian/Fair Isaac Model by End User during the term of this agreement.

C. **Term**. Annual Membership

2. Experian/Fair Isaac Scores

A. **Generally**. Upon request by End User during the Term, Provider will provide End User with the Scores.

B. **Time of Performance**. Instant access through membership.

C. **Warranty**. Provider warrants that the Scores are empirically derived and statistically sound predictors of consumer credit risk on the data from which they were developed when applied to the population for which they were developed. Provider further warrants that so long as it provides the Scores, the Scores will not contain or use any prohibited basis as defined by the federal Equal Credit Opportunity Act, 15 USC Section 1691 et seq. or Regulation B promulgated thereunder. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES PROVIDER HAS GIVEN END USER WITH RESPECT TO THE SCORES, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, PROVIDER MIGHT HAVE GIVEN END USER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OF FITNESS FOR A PARTICULAR PURPOSE. End User's rights under the foregoing warranties are expressly revalidation of the Experian/Fair Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 et seq.).

D. **Release**. End User hereby releases and holds harmless Provider, Fair Isaac and/or Experian and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-part contractors or suppliers of Provider, Fair Isaac or Experian from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered of incurred by End User resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.

3. **Fees**. Included in cost of report.

4. Intellectual Property

A. **No License**. Nothing contained in this Agreement shall be deemed to grant End User any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by Provider, Experian and/or Fair Isaac or any third party involved in the delivery of the scoring services hereunder. End User acknowledges that the Experian/Fair Isaac Model and its associated intellectual property rights in its output are the property of Fair Isaac.

B. **End User Use Limitations**. By providing the Scores to End User pursuant to this Agreement, Provider grants to End User a limited license to use information contained in reports generated by the Experian/Fair Isaac Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing Provider to deliver Scores to any third party (as may be permitted by this Agreement), End User agrees to enter into a contract with such third party that (1) limits use of the Scores by the third party only to the use permitted to the End User, and (2) identifies Experian and Fair Isaac as express third party beneficiaries of such contract.

C. **Proprietary Designations**. End User shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names or any other proprietary designations of Provider, Experian or Fair Isaac or their respective affiliates, whether registered or unregistered, without such party's prior written consent.

5. Compliance and Confidentiality

A. **Compliance with Law**. In performing this Agreement and in using information provided hereunder, End User will comply with all Federal, state, and local statutes, regulations, and rules applicable to consumer credit information and nondiscrimination in the extension of credit from time to time in effect during the Term. End User certifies that (1) is has a permissible purpose for obtaining the Scores in accordance with the federal Fair Credit Reporting Act, and any similar applicable state statute, (2) an use of the Scores for purposes of evaluating the credit risk associated with applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act, and (3) the Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the End User along with the Scores.

B. **Confidentiality**. End User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. End User will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate

business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, End User will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of End User and while in transport between the parties. End User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian's and Fair Isaac's express written permission.

C. **Proprietary Criteria**. Under no circumstances will End User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair Isaac in performing the scoring services hereunder.

D. **Consumer Disclosure**. Notwithstanding any contrary provision of this Agreement, End User may disclose the Scores provided to End User under this Agreement (1) to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only, and (2) as clearly required by law.

6. Indemnification and Limitations

A. **Indemnification of Provider, Experian and Fair Isaac**. End User will indemnify, defend, and hold each of Provider, Experian and Fair Isaac harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses (including attorneys' fees) arising out of or resulting from any nonperformance by End user of any obligations to be performed by End user under this Agreement, provided that Experian/Fair Isaac have given End User prompt notice of, and the opportunity and the authority (but not the duty) to defend or settle any such claim.

B. **Limitation of Liability**. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL PROVIDER, EXPERIAN OR FAIR ISAAC HAVE ANY OBLIGATION OR LIABILITY TO END USER FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY END USER, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER OR NOT END USER WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF PROVIDER, EXPERIAN OR FAIR ISAAC TO END USER EXCEED THE FEES PAID BY END USER PURSUANT TO THIS AGREEMENT DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF END USER'S CLAIM.

7. Miscellaneous

A. **Third Parties**. End user acknowledges that the Scores results from the joint efforts of Experian and Fair Isaac. End user further acknowledges that each Experian and Fair Isaac have a proprietary interest in said Scores and agrees that either Experian or the Fair Isaac may enforce those rights as required.

B. **Complete Agreement**. This Agreement sets forth the entire understanding of End User and Provider with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by an officer, employee, or representative of either party relating thereto.

IN WITNESS WHEREOF, End User and Provider have signed and delivered this Agreement.

PROVIDER:
Innovative Credit Solutions, Inc.
P O Box 1440
Lexington, SC 29071
800-345-2746

ENDUSER:
Business Name: _____

Contact Name (please print): _____

Signature: _____Date: _____

INNOVATIVE CREDIT SOLUTIONS, INC.

PHONE: 1-800-345-2746 FAX: 1-888-571-7222

END USER CERTIFICATION OF USE FOR EMPLOYMENT INSIGHT REPORTS

In compliance with the Federal Fair Credit Reporting Act as amended by the Consumer Credit Reporting Reform Act of 1996 (the "Act"), _____ ("End User") hereby certifies to Innovative Credit Solutions that it will comply with the following provisions:

1. End User will ensure that prior to procurement or causing the procurement of a consumer report for employment purposes (an Employment Insight Report):
    a. 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 for employment purposes; and
    b. The consumer has authorized in writing the procurement of the report by the End User.

2. In using a consumer report for employment purposes, before taking any adverse action based in whole or in part on the report, the End User shall provide to the consumer to whom the report relates:
    a. A copy of the report; and
    b. A description in writing of the rights of the consumer under the Act, a copy of which is attached hereto ("Summary of Consumer Rights").

The information from the consumer report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

End User hereby acknowledges receipt of the Summary of Consumer Rights.

_____
End User - Company Name

_____
Print Name

_____ _____
Signature Date

_____
Title

INNOVATIVE CREDIT SOLUTIONS
EXHIBIT A
END USER CERTIFICATION OF COMPLIANCE
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, _____ ("End User") hereby certifies to Consumer Reporting Agency as follows:

(Please circle)
End User ***(IS) (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.

_____
End User

By:_____

Title:_____

Date:_____

EXHIBIT B
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 person required to obtain consumer consent pursuant to 9V.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.

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.

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.

The undersigned _____ ("Subscriber"), acknowledges that it subscribes to receive various information services from Innovative Credit Solutions ("ICS") 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 counter parts. In connection with Subscriber's continued use of ICS information services in relation to Vermont consumers, Subscriber hereby certifies as follows:

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

Subscriber: _____
(please print)

Signed By: _____

Printed Name: _____

Title: _____

Date: _____

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Report Act (FCRA) is designed to promote accuracy, fairness, and privacy of information used in the process of granting credit. This information is supplied by public record sources, credit grantors and others to credit reporting agencies (CRA's) who organize and store that information for distribution to credit grantors, employers and insurers who are making credit, employment and insurance decisions about you. The FCRA gives suppliers and users of credit information, and CRA's specific responsibilities in connection with their respective roles in the credit granting and reporting process. The FCRA also gives you specific rights in dealing with these entities, as summarized below. You can find the complete text of the FCRA, 15 U.S.C. 1681 et seq., at the Federal Trade Commission's web site (http://www.ftc.gov). You may have additional rights under state law. You may contact a state or local consumer protection agency or a state attorney general to learn those rights.

- Access to your file is limited. Your file may only be accessed by those who have a permissible purpose recognized by the FCRA – usually to consider an application you have submitted to a creditor, insurer, employer, landlord, or other business, or to consider you for an unsolicited offer of credit.

- Your consent is required for reports that are provided to employers or that contain medical information. A CRA may not give a report about you to your employer, or prospective employers without your written consent. A CRA may not report medical information about you to creditors, insurers, or employers without your permission.

- You can find out what is in your file. Upon your request a CRA must give you all the information in your file, and a list of everyone who has requested it recently. However, you are not entitled to any information concerning "risk scores," "credit scores," or other economic predictors that are in your file. There is no charge for the report if a third party used the information in your file to take unfavorable action toward you and you request the report with 60 days of receiving notice that the information in your file was used by a third party unfavorably. You are also entitled to one free report every twelve months upon request if you certify that (1) you are unemployed and plan to seek employment within 60 days, (2) you are on welfare, or (3) your report is inaccurate due to fraud. Otherwise, a CRA may charge you a fee of up to eight dollars.

- You must be told if information in your file was a factor considered by a third party who took unfavorable actions toward you. Upon your request, anyone who considers information from a CRA and who takes unfavorable actions toward you—such as denying an application for credit, insurance, or employment—must give you the name, address, and phone number of the CRA that provided the information. Keep in mind that the third party, not the CRA, took the unfavorable action toward you and that the CRA will not be able to provide you with the reason for the unfavorable action.

- You can dispute inaccurate information with the CRA. If you tell a CRA that your file contains inaccurate information, the CRA must reinvestigate the items (usually within30 days) by presenting to its information source all relevant evidence you submit, unless your dispute is frivolous. The source must review your evidence and report its findings to the CRA. (The source also must advise national CRA's—to which it has provided data—of any error.) The CRA must give you a written report of the investigation, and a copy of your report if the investigation results in any change. If the CRA's investigation does not resolve the dispute, you may add a brief statement to your file. The CRA must normally include a summary of your dispute statement in future reports. If an item is deleted or a dispute statement is filed, you may ask that anyone who has recently received your report be notified of the change.

- Inaccurate information must be corrected or deleted. A CRA must remove inaccurate information from its files, usually within 30 days after you dispute it. However, the CRA is not required to remove accurate date from your file unless it is outdated (as described below) or cannot be verified. If your dispute results in any change to your report, the CRA cannot reinsert into your file a disputed item unless the information source verifies its accuracy and completeness. In addition, the CRA must give you a written notice telling you it has reinserted the

item. The notice must include the name, address and phone number of the information source.

- You can dispute inaccurate items with the source of the information. If you tell the third party who furnished information to a CRA—such as a creditor who reports to a CRA—that you dispute an item, it may not then report the information to a CRA without including a notice of your dispute. In addition, once you've notified the source of the error in writing, it may not continue to report the information if it is in fact an error.

- Outdated information may not be reported. In most cases, a CRA may not report negative information that is more than seven years old (ten years for bankruptcies).

- You may choose to exclude your name from CRA lists for unsolicited credit and insurance offers. Creditors and insurers may use file information as the basis for sending you unsolicited offers of credit or insurance. Such offers must include a toll-free telephone number for you to call and tell the CRA if you want your name and address removed from future lists or offers. If you notify the CRA through the toll-free number, if must keep you off the lists for two years. If you request, complete and return the CRA form provided for this purpose, you can have your name and address removed indefinitely.

- You may seek damages from violators. If a CRA, a user or (in some cases) a provider of CRA data, violates the FCRA, you may sue them in state or federal court.

The FCRA gives several different federal agencies authority to enforce the FCRA:

CRA's, creditors and others not listed below	Federal Trade Commission Bureau of Consumer Protection – FCRA Washington, DC 20580 ● 202-326-3761
National banks, federal branches/agencies of foreign banks (word "National" or initials "N.A." appear in or after bank's name	Office of the Comptroller of the Currency Compliance Management, Mail Stop 6-6 Washington, DC 20219 ● 202-452-3693
Federal Reserve System member banks (except national banks, and federal branches/agencies of foreign banks)	Federal Reserve Board Division of Consumer & Community Affairs Washington, DC 20551 ● 202-452-3693
Savings associations and federally chartered savings banks (word "Federal" or initials "F.S.B." appear in federal institution's name)	Office of Thrift Supervision Consumer Programs Washington, DC 205520 ● 800-842-6929
Federal credit unions (words "Federal Credit Union" appear in institution's name)	National Credit Union Administration 1775 Duke Street Alexandria, VA 22314 ● 703-518-6360
Banks that are state-chartered, or are not Federal Reserve System members	Federal Deposit insurance Corporation Division of Compliance & Consumer Affairs Washington, DC 20429 ● 800-934-FDIC
Air, surface, or rail common carriers regulated by former Civil Aeronautics Board or Interstate Commerce Commission	Department of Transportation Office of Financial Management Washington, DC 20590 ● 202-366-1306