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 *TransUnion* bureau. Please read, fill out and sign the application completely (pages 1 through 11). Your signature acknowledges you have read and will comply with the provisions within these documents. Please include all required documentation and email or fax the completed application.

- All pages must be signed and completed (no exceptions). Please make sure the credit card information is correct.
    - Pages 1 & 2 – Application Form – you may enter the information electronically or a hand-written copy is acceptable. Please complete all information. Make sure the credit card information is correct and the page is signed.
    - Pages 3 & 4 – Broker Subscriber Agreement – top of page 3 – print the name of your company in the blank; bottom of page 4 – print your name & company name; sign & date
    - Page 5 – FCRA Requirements – print your company name (End User), your name and title; sign & date
    - Pages 6 to 10 – Access Security Requirements – page 10 – print your company name and your name, sign & date
    - Page 11 – Subscriber Agreement for Employment purposes – top of page - enter the name of your company; bottom of page - enter your name & company name; sign & date

- 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.

- We will need a telephone number and contact person that can be reached during the day. An e-mail address 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 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.

Email: info@icscredit.com
Fax: 888-571-7222

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:

Disclaimer of Warranty: Because this service involves information provided from other sources, Innovative Credit Solutions, Inc. cannot and will not be an insurer or guarantor of the accuracy of reliability of the service of data released or stored. Innovative Credit Solutions does not guarantee or warrant the accuracy, timeliness, completeness, currentness, merchantability or fitness for a particular purpose of the service. Information in the service or the media on or through which the services are provided and shall not be liable to Subscriber or to any of the Subscribers customers for any loss or injury arising out of or caused in whole or part by Innovative Credit Solutions, Inc. acts or omissions, whether negligent or otherwise, in procuring, compiling, collecting, interpreting, reporting, communicating or delivering the services or information therein.

Company Name				
Specific purpose(s) for which Consumer Reports will be used				
Is the company engaged in the underwriting of insurance? ☐ Yes ☐ No				
Is the company licensed or providing service as an attorney or detective/investigative agency? ☐ Yes, if so please check appropriate service ☐ Attorney or ☐ Detective/Investigative Agency ☐ No				
Does the company intend to resell or release information from the consumer credit report to a third party? ☐ Yes ☐ No				
Will the company or does the company provide credit repair or credit counseling services for a fee? ☐ Yes ☐ No				
Estimated number of reports to be used monthly				
Will the company access consumer reports: ☐ Locally ☐ Regionally ☐ Nationally				
BANK REFERENCE				
Bank Name			Phone:	
BUSINESS REFERENCES				
Business Name	City	State	Phone	
Check the appropriate business structure: ☐ Sole Proprietorship ☐ Partnership ☐ Corporation ☐ Other				
Complete for Sole Proprietor or Partnership				
Owner #1 Name			Social Security #	
Resident Street Address				
City	State	County	Zip	
Signature				
Owner #2 Name			Social Security #	
Resident Street Address				
City	State	County	Zip	
Signature				
Complete for Corporation				
Officer Name			Title	
Officer Name			Title	
Officer Name			Title	
SIGNATURE & AGREEMENT				
I certify that the information provided on this application is true. I understand by the signature below that you may pull a personal credit report on owners of this company for use in processing this Application for Service.				
Signature			Date	
Print Name			Title	

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 available at www.icscredit.com.

Recognizing that information obtained through ICS is secured by and through fallible human sources and that, for the fee charged, ICS, TransUnion, 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, Trans Union, Equifax or Experian and Subscriber releases ICS, TransUnion, 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 Isaac, ICS, TransUnion, 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, TransUnion, Equifax or Experian do not guarantee the predictive value of a score. Subscriber releases ICS, TransUnion, 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.

It is also understood and agreed that random audits will be conducted to ensure that the Subscriber is in compliance with the FCRA and other certifications in this agreement. Audits will be conducted by mail when possible and the Subscriber will be required to provide documentation to show permissible use of the particular consumer report. Subscriber agrees that any failure to show permissible use for a consumer report will be a breach in this agreement and is grounds for suspension of service or termination of this agreement.

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 five (5) 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. 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, imprisoned for not more than 2 years, or both.

Subscribers may discuss information obtained through ICS with the consumer in the event Subscriber declines or takes adverse action regarding the consumer. ICS, TransUnion, 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. Whenever credit or insurance for personal, family, or household purposes, or employment involving a consumer is denied or the charge for such credit or insurance is increased either wholly or partly because of information contained in a consumer report from a consumer reporting agency, the user of the consumer report shall so advise the consumer against whom such adverse action has been taken and supply the name and address of the consumer reporting agency making the report.

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).

You acknowledge you will not take any adverse action against any consumer without further investigation to verify the information from the DMF.

By signing below Subscriber acknowledges that Subscriber has read, 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 _____

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 at website: http://www.ftc.gov/os/statutes/031224fcra.pdf 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.

Subscriber: _____

SIGNATURE_____ DATE _____

PRINT NAME_____

TITLE _____

Access Security Requirements

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to Consumer 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 Consumer 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 Consumer 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 Consumer 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 Consumer 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 Consumer 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 Consumer 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 Consumer data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Consumer 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 Consumer 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 Consumer data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

4. Maintain an Information Security Policy

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

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable 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 Consumer 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 Consumer data, ensure that service provider is compliant with Consumer Independent Third Party Assessment (EI3PA) program, and registered in Consumer 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 Consumer 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 Consumer 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 Consumer 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 Consumer data on mobile devices is prohibited. Any exceptions must be obtained from Consumer 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 Consumer 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 Consumer 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 Consumer 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 Consumer:
  - 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 Consumer 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 Consumer 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 Consumer 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 Consumer 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 Consumer 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, Consumer 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, Consumer 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 Consumer 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: _____

INNOVATIVE CREDIT SOLUTIONS, INC.
SUBSCRIBER AGREEMENT
For Employment Purposes

This Agreement is made and entered into as of _____ ("Effective Date"), by and between Innovative Credit Solutions and (Company Name) _____ (Company Address) _____.

End User is a (type of business) _____ and has a need for consumer credit information in connection with the evaluation of individuals for employment, promotion, reassignment or retention as an employee ("Consumer Report for Employment Purposes").

End User shall request Consumer Report for Employment Purposes pursuant to procedures prescribed by Reseller from time to time only when it is considering the individual inquired upon for employment, promotion, reassignment or retention as an employee, and for no other purpose. End User shall comply with any federal and state laws which may restrict or ban the use of Consumer Report for Employment Purposes.

End User certifies that it will not request a Consumer Report for Employment Purposes unless:

a. A clear and conspicuous disclosure is first made in writing to the consumer by End User before the report is obtained, in a document that consists solely of the disclosure that a consumer report may be obtained for employment purposes;
b. The consumer has authorized in writing the procurement of the report; and
c. Information from the Consumer Report for Employment Purposes will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

End User further certifies that before taking adverse action in whole or in part based on the Consumer Report for Employment Purposes, it will provide the consumer with:

a. A copy of the Consumer Report for Employment Purposes; and
b. A copy of the consumer's rights, in the format approved by the Federal Trade Commission.

End User shall use the Consumer Report for Employment Purposes only for a one-time use, and shall hold the report in strict confidence, and not disclose it to any third parties that are not involved in the employment decision.

End User will maintain copies of all written authorization for a minimum of five (5) years from the date of inquiry.

With just case, such as violation of the terms of End User's contract or a legal requirement, or a material change in existing legal requirements that adversely affects End User's Agreement, Reseller may, upon its election, discontinue serving the End User and cancel the agreement immediately.

NOTE: The Consumer Report for Employment Purposes provided by Trans Union to the Reseller may contain the consumer's date of birth, which is only to be used for Reseller's internal identity verification purposes. Neither the year of birth, nor the consumer's age, may be passed on to an End User under any circumstance in the Consumer Report for Employment purposes.

Reseller: Innovative Credit Solutions

Signature: _____

Printed Name: _____

Title: _____ Date: _____

End User Company Name: _____

Signature: _____

Printed Name: _____

Title: _____ Date: _____