

***Company Information***

Business Name (End-User)			
Street Address	City	State	Zip
SSN or Federal Id Number	Year Business Established	Is this a <u>Residential</u> Address? <input type="checkbox"/> Yes <input type="checkbox"/> No	
Main Contact	Title	Business Phone	
Email Address & Web Site:			Business Fax

***Business References***

Business Reference (Name/Company/Title)	Contact Number
Business Reference (Name/Company/Title)	Contact Number
Business Reference (Name/Company/Title)	Contact Number

***Electronic Invoice***

Primary Billing Contact Name	Primary Billing Contact Email	Primary Billing Contact Phone
Secondary Billing Contact Name(s) – you may enter multiple contacts		Secondary Billing Contact Emails
Pay by Credit Card ( <i>optional</i> ) Complete the following if you prefer to have your monthly charges applied to a card.		
Card Type: <input type="checkbox"/> Visa <input type="checkbox"/> MasterCard <input type="checkbox"/> American Express		
Card Number:	Expiration Date:	
Name on Card:	Signature:	

***Permissible Purpose/Compliance Information***

<p>Please indicate your company's business type and your intended use of credit reports and related products and services</p> <p><b>Type of Business:</b></p> <p><b>Intended Use of Consumer Information:</b></p> <p><b>Please fax the following to 888-216-1003:</b></p> <p><input type="checkbox"/> A copy of your advertising material/business card</p> <p><input type="checkbox"/> A copy of a business check – <b>or</b></p> <ul style="list-style-type: none"> <li>- a letter from bank confirming business checking account - <b>or</b></li> <li>- signed authorization for us to confirm your business checking account</li> </ul>
---



## Service Agreement

This service agreement ("Agreement") is entered into as of the date written below between ScreeningONE, Inc. ("ScreeningONE"), and \_\_\_\_\_ ("Client").

Client and ScreeningONE agree to the following terms:

1. Pricing: Set forth on the attached price list.
2. Client is familiar with the requirements of all applicable federal and state laws, including the Fair Credit Reporting Act ("FCRA") and the Fair and Accurate Credit Transactions ("FACT") Act, including without limitation the provisions set forth herein, and Client agrees to comply with all requirements of these laws in connection with ordering and using Consumer Reports and related products and services ("Consumer Reports"). Client agrees that it is solely responsible for this compliance. Client acknowledges that it has received and read the acknowledgement and access security requirements documents provided by ScreeningONE.
3. Client will order Consumer Reports and related products and services for its exclusive use only, solely for permissible purposes as defined by federal and state law. Client certifies that it will be the end user of all Consumer Reports and agrees that it will hold all information strictly confidential, and will not copy, sell or transfer any such information to any third party. Client agrees to implement appropriate procedures so that only employees with adequate training regarding the requirements of the FCRA, FACT Act and all applicable federal and state laws have access to the Consumer Reports.
4. Client will obtain a signed authorization from each person on whom Consumer Report is ordered (the "Subject"), prior to ordering a Consumer Report on such Subject, and will maintain the authorization on file for audit and inspection. This requires Client to maintain a clear copy of photographic identification of each Subject along with the authorization for three years. During this period, Client will provide ScreeningONE with a copy of such authorization, or the original, as may be requested by ScreeningONE or its authorized representatives. Client agrees that ScreeningONE, upon reasonable notice, may conduct audits to ensure Client's compliance with the FCRA, FACT Act and all applicable federal and state laws, and requirements of this Agreement, and Client agrees to provide reasonable cooperation with ScreeningONE in connection with such audits.
5. Client certifies that it has a permissible purpose for obtaining a Consumer Report as follows:
  - EMPLOYMENT SCREENING: Client is an employer and has a need for consumer credit information in connection with the evaluation of individuals for employment.**
  - TENANT SCREENING: Client is a property management company and/or property owner and has a need for consumer credit information in connection with the evaluation of individuals as tenants.**
  - OTHER: Please indicate (1) your company's business and (2) your intended use of Consumer Reports and related products and services from ScreeningONE:**
6. Client certifies that it will request Consumer Reports only for the permissible purpose certified above, and will use the reports obtained for no other purpose.
7. Consumer Reports will be requested only by Client's designated representatives. Employees and/or agents of Clients are forbidden to attempt to obtain or obtain reports on themselves, associates, or any other person except in the exercise of their official duties and in compliance with the law.
8. THE LAW PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER FEDERAL LAW OR IMPRISONED, OR BOTH.
9. Client's account is delinquent if not paid in full within 30 days from the date of the invoice. Client is responsible for a finance charge of 10 percent per annum (or the highest rate allowable by law) on all delinquent amounts until paid.
10. Client shall pay to ScreeningONE reasonable attorneys' fees and costs incurred by ScreeningONE in collecting a delinquent account, or to otherwise enforce the terms of this agreement, including permissible purpose compliance, whether or not litigation is instituted. In the event of any litigation or other action involving this Agreement, the prevailing party shall be paid reasonable attorneys' fees and costs.



11. This Agreement contains the entire understanding and agreement between ScreeningONE and the Client and no other representations, covenants, undertakings or other prior or contemporaneous agreements, oral or written, respecting such matters, which are not specifically incorporated herein, shall be deemed in any way to exist or bind ScreeningONE or the Client. ScreeningONE and the Client acknowledge that they have not executed this agreement in reliance on any such promise, representation or warranty. This Agreement shall not be modified by any oral representation made before or after the execution of this agreement. All modifications must be in writing and signed by both ScreeningONE and the Client.

12. Client agrees to use ScreeningONE as its sole and exclusive provider of Consumer Reports and related products and services for a minimum term of twelve (12) months. This agreement shall automatically renew for additional periods of twelve (12) months each, unless either party gives written notice to the other party at least 60 days in advance. This notice must be received by ScreeningONE via certified mail, fax or e-mail. In the event of an agreed upon trial period, which agreement shall be in writing, the trial period shall begin from the date that the Client runs its first Consumer Report through ScreeningONE.

13. Client shall indemnify and hold harmless ScreeningONE, and each of its affiliated persons and entities, from and against any and all liability, losses, claims, damages, and expenses, including, but not limited to, attorneys' fees and court costs, arising from or in any way connected with any breach or claimed breach of the terms of this Agreement by Client or any third person, including any representation, warranty, covenant, or agreement herein including, without limitation, any improper publication or disclosure or other misuse of a Consumer Report or information by Client or any third person or entity, including in violation of federal or state law.

14. This Agreement and the covenants and conditions contained herein shall apply to, be binding upon and transfer to the benefit of the administrators, executors, legal representatives, assignees, successors, agents and assigns of ScreeningONE and Client. This Agreement shall be governed by and construed in accordance with California law.

15. The pricing set forth in this Agreement (including the attached pricing list) is based on the pricing agreement for Consumer Reports and/or related products and services presently in place between ScreeningONE and the credit repositories (the "Repositories"), and/or their authorized brokers/resellers. Accordingly, notwithstanding any other term in this agreement, ScreeningONE's provision of Consumer Reports and/or related products and services to Client may be terminated immediately if the Repositories terminate ScreeningONE's ability to provide Consumer Reporting services. In the event that the Repositories increase the price of Consumer Reports and/or related products and services to ScreeningONE, ScreeningONE, at its option, may pass on the price increase to the Client, or terminate the provision of Consumer Reports and/or related products and services to Client.

16. In the event that Client fails to pay any invoice when due, Client hereby grants to ScreeningONE and/or its affiliated agents or companies the right to receive direct payment for all amounts due directly from Client's checking or credit accounts. Client hereby grants ScreeningONE a power of attorney, coupled with an interest, such that ScreeningONE can instruct checking and credit accounts to pay invoices due.

17. Client must conform to the SUBSCRIBER CERTIFICATION OF COMPLIANCE pursuant to California Civil Code section 1785.14 (a).

***Please check the appropriate box:***

**Client**  *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").**

18. Client agrees to each of the forgoing terms. By signing below, the following person declares and attests under the laws of the United States that the foregoing, and the information and documents provided with the application, are true and correct.

Name (Printed): \_\_\_\_\_ Position: \_\_\_\_\_

Signature: \_\_\_\_\_ Date: \_\_\_\_\_



**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 ScreeningONE 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.

\_\_\_\_\_  
Name of End User Company (Client)

\_\_\_\_\_  
Printed Name of End User Representative

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

## Access Security Requirements

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. *We recognize that all of the items or terms identified in this document may not necessarily apply to each end user.* If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. Capitalized terms used herein have the meaning given in the Glossary attached hereto. Experian reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides a baseline for information security.

In accessing Experian's services, please make sure you are familiar with these security requirements:

### **1. Implement Strong Access Control Measures**

- 1.1 Do not provide your Experian Subscriber Codes or passwords to anyone. No one from Experian will ever contact you and request your Subscriber Code number or password.
- 1.2 Proprietary or third party system access software must have Experian Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.
- 1.3 You must request your Subscriber Code password 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 of
- 1.4 Protect Experian Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).
- 1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to Experian's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 Develop strong passwords that are:
  - Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
  - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.
- 1.13 Ensure that you and your employees do not access your own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.
- 1.14 Implement a process to terminate access rights immediately for users who access 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.

- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

## **2. Maintain a Vulnerability Management Program**

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

## **3. Protect Data**

- 3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)
- 3.2 All Experian data is classified as Confidential and must be secured to this requirement at a minimum.
- 3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 3.4 Encrypt all Experian data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

**4. Maintain an Information Security Policy**

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 4.2 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- 4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

**5. Build and Maintain a Secure Network**

- 5.1 Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
- 5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
- 5.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- 5.4 Any stand alone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.
- 5.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

**6. Regularly Monitor and Test Networks**

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access Experian systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:
  - protecting against intrusions;
  - securing the computer systems and network devices;
  - and protecting against intrusions of operating systems or software.

**Record Retention:** *The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, 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 \$2,500 per violation.”*

Client Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**Glossary**

<b>Term</b>	<b>Definition</b>
<b>Computer Virus</b>	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.
<b>Confidential</b>	Very sensitive information. Disclosure could adversely impact your company.
<b>Encryption</b>	Encryption is the process of obscuring information to make it unreadable without special knowledge.
<b>Firewall</b>	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.
<b>Information Lifecycle</b>	(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.
<b>IP Address</b>	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.
<b>Peer-to-Peer</b>	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.
<b>Router</b>	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.
<b>Spyware</b>	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.
<b>SSID</b>	Part of the Wi-Fi Wireless LAN, a service set identifier (SSID) is a code that identifies each packet as part of that network. Wireless devices that communicate with each other share the same SSID.
<b>Subscriber Code</b>	Your seven digit Experian account number.
<b>WEP Encryption</b>	(Wired Equivalent Privacy) A part of the wireless networking standard intended to provide secure communication. The longer the key used, the stronger the encryption will be. Older technology reaching its end of life.
<b>WPA</b>	(Wi-Fi Protected Access) A part of the wireless networking standard that provides stronger authentication and more secure communications. Replaces WEP. Uses dynamic key encryption verses static as in WEP (key is constantly changing and thus more difficult to break than WEP).