



Sign Up Instructions

For an Individual Landlord

To subscribe to CIC's services, simply fax or mail the following documents:

- Completed Subscriber Service Application & Agreement (4 pgs.)
- Credit Card Agreement
- "FCRA and Access Security Requirements" signed acknowledgment

For more information, contact: **888-316-4242**
info@cicreports.com

Authorized ILA Resident Screener. Thank you for supporting your local association!



Contemporary Information Corporation
42913 Capital Drive, Unit 101 Lancaster, CA 93535
Phone 888-316-4242 Fax 661-974-8019



INDIVIDUAL LANDLORD

SUBSCRIBER SERVICE APPLICATION AND AGREEMENT
PLEASE PROVIDE ALL OF THE INFORMATION REQUESTED BELOW.

SUBSCRIBER

Last Name First Name MI
DOB Social Security Number Drivers License
Address City State Zip
Home Phone Number Business Phone Number
Fax Number Email Address

EMPLOYMENT

Company Name Phone Number
Address City State Zip
Position Supervisor
Salary Length of Employment

BANK REFERENCE

Bank Name Branch Phone Number
Checking Acct No. Savings Acct No.
Average Balance Date Opened

CO-SUBSCRIBER

Last Name First Name MI
DOB Social Security Number Drivers License
Address City State Zip
Home Phone Number Business Phone Number
Fax Number Email Address

EMPLOYMENT

Company Name Phone Number
Address City State Zip
Position Supervisor
Salary Length of Employment

BANK REFERENCE

Bank Name Branch Phone Number
Checking Acct No. Savings Acct No.
Average Balance Date Opened

Please indicate the addresses of the properties that you own or manage:

Please indicate on the line below, the specific purpose for which credit reports, motor vehicle reports and/or other information regulated by the Fair Credit Reporting Act (FCRA) will be used:





SUBSCRIBER SERVICE AGREEMENT

CONTEMPORARY INFORMATION CORP. (CIC) AND SUBSCRIBER AGREE AS FOLLOWS:

- 1. CIC SERVICES.** On request, CIC shall furnish to Subscriber and to Subscriber's designated agents and employees, information and data stored in CIC's computerized reporting system(s) and provided to CIC by credit and other information reporting services. Subscriber's request for information and data shall identify the business purpose and other information concerning Subscriber as may be required by CIC. CIC shall furnish information in oral, written or computerized form.
- 2. CHARGES TO SUBSCRIBER.** For each response to a request for information (including a "no record found" response), Subscriber agrees to pay CIC the applicable charges then prevailing for the service rendered to Subscriber and to Subscriber's agents and employees. In the event of any sale of property, or change in the identity of Subscriber's agents or employees authorized to order information from CIC, Subscriber shall notify CIC in writing. Subscriber shall be liable for charges incurred by Subscriber's agents and employees, and with respect to Subscriber's properties until the date on which CIC receives said notice. The amount of charges will be specified in CIC's price schedule and are subject to change on thirty (30) days written notice to Subscriber. Payment by Subscriber shall be due upon receipt of the invoice unless other arrangements are made, in writing, with the finance department of CIC. Unpaid invoices more than thirty (30) days old shall bear interest from the date of the invoice at the rate of twelve percent (12%) per annum, until paid. CIC may suspend Subscriber's account for non-payment after forty-five (45) days from invoice due date. In such an event, Subscriber understands that it must pay a \$25.00 account re-activation fee, along with all past due balances to reinstate said account.
- 3. CIC PERFORMANCE.** CIC will use its best efforts to maintain and regularly augment its compilation of information and to obtain accurate information from credit reporting services. CIC will exercise its best efforts to obtain and provide the information requested by Subscriber in an expeditious and efficient manner. Subscriber is aware that because of similar names, delays mandated by law in providing information, and errors and oversights by third parties and others in connection with assembling, recording and providing information, CIC cannot and does not in any fashion guaranty the accuracy of information submitted.
- 4. LIMITATION OF LIABILITY.** The low cost of the information provided by CIC precludes CIC from acting as an insurer for losses which may result from any inaccuracy in reporting. Subscriber agrees that the Subscriber's actual damage which may be sustained by reason of any inaccuracy in a report or other failure of CIC would be impracticable or extremely difficult to fix, and damages for which CIC shall be liable shall be limited to and not exceed the cost of the service provided. In no event shall CIC be responsible for any damage, whether consequential, incidental or otherwise (including without limitation any loss of profit or revenues), incurred by Subscriber in excess of the cost of the service provided by CIC.
- 5. ARBITRATION.** Any controversy or dispute between the parties involving the construction or application of any of the terms, covenants or conditions of this agreement, or arising by reason of the alleged breach or default of any party hereunder, shall be submitted to arbitration before the American Arbitration Association in Los Angeles, California, on the request of any party. Arbitration shall be governed by the provisions of the Commercial Arbitration Rules then in effect. Any reward rendered in such Arbitration may, at the discretion of the arbitrator, allocate to the prevailing party and against the losing party all costs of arbitration including filing fees and arbitrator's compensation. Notwithstanding the foregoing, and without waiving the obligation to arbitrate all other controversies and disputes, CIC shall not be required to arbitrate claims for unpaid invoices which total less than \$2,500, but, may pursue such claims by legal action.
- 6. SUBSCRIBER USE LIMITATIONS.** Subscriber is aware that credit and public record information is or may be claimed to constitute confidential information concerning the individual or business for whom information is requested. For that reason, Subscriber hereby certifies and agrees that it will request and or use information received from CIC solely in connection with transactions involving the extension of credit to the consumer or the business as to whom information is sought, and Subscriber will not request or use such information for any purpose prohibited by law. All information provided by CIC to Subscriber shall be retained by Subscriber in strict confidence and disclosed only to employees and agents whose duties reasonably relate to legitimate business purposes for which information is requested. Subscriber agrees that Subscriber shall not sell or otherwise distribute to any third party any information received hereunder, except as otherwise provided by this agreement or required by law. Subscriber understands that it cannot access consumer credit information on its employees, or on itself. Subscriber further understands that CIC's services can only be used for the purpose(s) that Subscriber indicated on Subscriber Service Application.



7. FCRA AND ACCESS SECURITY REQUIREMENTS. Subscriber has read and understands the “FCRA and Access Security Requirements / CIC Policies” and will take all reasonable measures to enforce the policies set forth therein. Subscriber certifies that it will use the information obtained from CIC for no other purposes than what is stated in this Application and Agreement and for the type of business listed on this Application. Subscriber will not sell information obtained from CIC to any consumer or business entity directly or indirectly. Subscriber understands that if its systems are used improperly by its personnel, or if subscriber access codes are made available to any unauthorized personnel due to carelessness on the part of any employee, officer, official or agent, Subscriber may be held responsible for financial losses, or monetary charges that may be incurred and that Subscriber’s access privileges may be terminated.

8. CRIMINAL RECORD PROVISIONS. If Subscriber accesses criminal record information through CIC it must meet the requirements as defined in the following statutes: Freedom of Information Act, 5 USC 552; Crime Control Act, Public Law 93-579, 5 USC 522(a), Title 6, Fair Credit Reporting Act, Public Law 91-508; and all other state and federal laws that are concerned with the reporting and use of criminal record information.

9. CREDIT SCORING PROVISIONS. Several information products furnished by CIC to Subscriber contain credit scores developed by the Fair Isaac model (FICO), Experian, TransUnion and Equifax (hereinafter referred to as “credit scores”). CIC and Subscriber agree on the following terms and conditions regarding credit scores:

- (i) Subscriber warrants that it has a “permissible purpose” under the Fair Credit Reporting Act (FCRA), as it may be amended from time to time, to obtain the information derived from credit scores;
- (ii) Subscriber agrees to limit its use of the credit scores and reason codes solely to use in its own business with no right to transfer or otherwise sell, license, sublicense or distribute said credit scores or reason codes to third parties;
- (iii) Subscriber will maintain internal procedures to minimize the risk of unauthorized disclosure and Subscriber agrees that credit scores and reason codes will be held in strict confidence and disclosed only to those of its employees with a “need to know” and to no other person;
- (iv) Subscriber will hold all credit scores in strict confidence and will not disclose any credit score to the consumer or to any third party except as required by law as a result of adverse action. Subscriber may provide the principal factors contributing to the credit scores to the subject of the report when those principal factors are the basis of Subscriber’s adverse action against the subject consumer;
- (v) Subscriber agrees to comply with all applicable laws and regulations in using credit scores and reason codes;
- (vi) Subscriber, its employees, agents or subcontractors are prohibited from using any trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of Experian Information Solutions, Inc., or of Fair Isaac and Company, or of TransUnion LLC or of Equifax Information Services, or of Contemporary Information Corp., or the affiliates of any of them, or of any other party involved in the provision of credit scores and other information without such entity’s prior written consent;
- (vii) Subscriber agrees that it will not attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used to develop the credit scores or the credit scoring system;
- (viii) Experian/Fair, Isaac warrants that the Experian/Fair Isaac Model is empirically derived and demonstrably and statistically sound and that to the extent the population to which the Experian/Fair Isaac Model is applied is similar to the population sample on which the credit scores were developed, the credit scores may be relied upon by the Subscriber to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to Subscriber. Experian/Fair, Isaac further warrants that so long as it provides the Experian/Fair Isaac Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC Section 1691 *et seq.* THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES EXPERIAN/FAIR, ISAAC HAVE GIVEN SUBSCRIBER WITH RESPECT TO THE EXPERIAN/FAIR, ISAAC MODEL AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED;
- (ix) The aggregate liability of Experian/Fair, Isaac, TransUnion, Equifax and CIC is limited to the lesser of the fees paid by Subscriber to obtain this information. Experian/Fair, Isaac, Equifax, and CIC are not liable for any incidental, indirect, special or consequential damages of any kind that may result from the use or reliance of credit scores.

10. ON SITE INSPECTION OF PREMISE. Subscriber agrees to a On Site Inspection of premise by a CIC approved vendor to validate the legitimacy and location of the business and to ensure security measures in restricting access to FCRA regulated information. Subscribers located out of a “residence” are required an annual On Site Inspection and will be billed at CIC’s prevailing rate. Subscribers located out of a “commercial” location are required the initial On Site Inspection and in the event the Subscriber relocates, a follow-up inspection will be performed and the Subscriber billed at CIC’s prevailing rate. In the event of a failed or no-show inspection, the account will still be charged.

Initials _____





11. **INDEMNIFICATION.** CIC shall indemnify, defend and hold Subscriber harmless from and against any and all costs, damages and liabilities (including reasonable attorney's fees actually incurred by Subscriber) which may be asserted against Subscriber based upon the improper use or distribution by CIC of information furnished by Subscriber to CIC. Subscriber shall indemnify, defend and hold CIC, Experian, TransUnion, Equifax and its agents harmless of and from any and all costs, demands and liabilities (including reasonable attorney's fees actually incurred by CIC) which may be asserted against CIC based upon Subscriber's improper use or distribution of information furnished to Subscriber by CIC. The indemnified party shall give prompt written notice to the indemnifying party of the receipt if any claim demand or liability to which the obligation of indemnification and hold harmless may apply.

12. **SEVERABILITY.** If any provision of this Agreement is held invalid or unenforceable by a court of competent jurisdiction, such invalidity or unenforceability shall have no effect upon other provisions of this agreement and shall remain fully valid, enforceable and binding on the parties.

13. **ENTIRE CONTRACT: CHOICE OF LAW.** This agreement sets forth the entire understanding and agreement between CIC and Subscriber and supersedes all prior and contemporaneous agreements, representations, and understandings of the parties; it may be modified only in written agreement duly executed by both parties. This Agreement shall be interpreted in accordance with the laws of the state of California as applied to contracts that are executed and performed entirely in California.

AUTHORIZATION

I/We certify the information is true and accurate. Contemporary Information Corporation or any firm acting in its behalf is hereby granted permission to perform a credit/investigative report on our company and/or its principals.

IN WITNESS WHEREOF, CIC and Subscriber have entered into this Agreement to be executed by their duly authorized representatives as of the date first written below.

SUBSCRIBER SIGNATURE **X** _____ Date _____
By (Print) _____ Title _____

CO-SUBSCRIBER SIGNATURE **X** _____ Date _____
By (Print) _____ Title _____

CONTEMPORARY INFORMATION CORP. (CIC)

SIGNATURE _____ Date _____
By (Print) Sabrina Bower Title Vice President

CONTEMPORARY INFORMATION CORPORATION
Nevada Private Investigator License #1588
42913 Capital Drive, Unit 101, Lancaster, CA 93535
Phone: (800) 288-4757 Fax: (661) 974-8019





CREDIT CARD AGREEMENT

In order to activate a new account or maintain an existing account, all subscribers must have a valid credit card on file with Contemporary Information Corporation (CIC). Therefore, subscriber agrees to the following terms and condition:

1. I authorize CIC to charge the credit card account and issuing financial institution, to pay all amounts due CIC. I agree that if any unsatisfied amount is referred to collection, I shall pay all reasonable collection costs, including attorney fees, and court costs.
2. If I chargeback a legitimate debt, than I agree to pay a chargeback fee of \$15.00 per transaction.
3. When the credit card expires or the card number changes, I am responsible for informing CIC.

AMERICAN EXPRESS MASTERCARD VISA

EXPIRATION DATE _____ CIC ACCOUNT #/CUSTOMER ID: _____
 SECURITY CODE _____

Please check this box if you would like to receive a copy of the invoice that was charged to your credit card.

Authorization Signature (“Subscriber”)

Signature

Print name as appears on card

Address

FCRA and Access Security Requirements / CIC Policies

IMPORTANT: PLEASE READ CAREFULLY!

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. Capitalized terms used herein have the meaning given in the Glossary attached hereto. The credit reporting agency reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security. ***In accessing the credit reporting agency's services, you agree to follow these security requirements:***

1. Implement Strong Access Control Measures

- 1.1 Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.
- 1.2 Proprietary or third party system access software must have credit reporting agency 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 credit reporting agency 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 the credit reporting agency'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 & letters)
 - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.
- 1.13 Ensure that you and your employees **do not access your own credit reports or those reports of any family member(s) or friend(s)** unless it is in connection with a credit transaction or for another permissible purpose.
- 1.14 Implement a process to terminate access rights immediately for users who access credit reporting agency credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

2. Maintain a Vulnerability Management Program

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

3. Protect Data

- 3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)
- 3.2 All credit reporting agency data is classified as Confidential and must be secured to this requirement at a minimum.
- 3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 3.4 Encrypt all credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at 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 credit reporting agency systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by: protecting against intrusions; securing the computer systems and network devices; and protecting against intrusions of operating systems or software.

7. FCRA & Other Policies

7.1 You must always get a subject's written authorization before accessing their credit and/or public record profile. If you access a subject's credit and/or public record information under false pretenses, and/or without their authorization the penalty for such action(s) under the Federal FCRA Section 621(a)(2)(A) is imprisonment for up to one year and up to a \$2,500 fine, and/or any civil damages the court may award the party which brought the action. **EXCEPTION: The Federal Fair Credit Reporting Act states in effect that a creditor or their authorized agent attempting to collect a valid and legally enforceable debt (with or without a judgment) from a subject, can obtain a credit profile on that subject without their authorization.**

7.2. **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 FCRA/FACTA, the credit reporting agency requires that you **retain the credit/rental application for a period of not less than 6 years (both approved and denied applicants).** When conducting an investigation, particularly following a breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.

7.3. **Adverse Action** - If you (or your client) deny a subject for a credit related transaction (in the form of a rental of a dwelling, the financing of a product or service, etc.) you are to provide them with such a notice in writing. This notice must reference the appropriate reporting agency, and state that the subject can request a copy of their credit profile from the credit reporting agency in question free of charge. They must request their credit profile within 60 days from the date they were denied credit (otherwise, they must pay the credit bureau's prevailing rate for a copy of their report). In addition, the notice must state that the subject has the right to dispute the accuracy or completeness of any information contained in their consumer credit and/or public record report.

7.4. **Prohibited Businesses** -CIC cannot serve any companies or individuals engaged in any of the following businesses: adult entertainment, businesses in an unrestricted residential location, attorneys or law offices, bail bondsman, check cashing, credit counseling or repair, dating service, financial counseling, genealogical research and people locator service, massage service, pawn shop, private detectives, 3rd party repossession, companies involved in spiritual counseling, future services (ex. health club, timeshare), tattoo service, news agencies, insurance claims, **those who intend to re-sell its credit and/or public record reports directly, or indirectly,** or those who plan to use (or which do use) such information in any unlawful manner as set forth in the Fair Credit Reporting Act, as well as any other applicable federal, state, and/or local laws(s). Furthermore, CIC cannot serve any individuals or companies which plan to use (or which do use) its reports for any purpose(s) prohibited by its policies and/or agreement. If you misuse said information in the manner(s) described above, your account with CIC will be terminated without notice.



Subscriber has read and understands the “**FCRA and Access Security Requirements/CIC Policies**” and will take all reasonable measures to enforce them.

Subscriber/Company

Authorized Signature

Print Name

Date

Resident Screening Reports

Online 24/7	ILA Member Price
Criminal Only	\$19 ⁰⁰
Social Search Only	\$6 ⁰⁰
Eviction + Social Search	\$10 ⁰⁰
Eviction + Social Search + Criminal	\$26 ⁰⁰

*Credit Only	\$15 ⁰⁰
*Credit + Eviction	\$22 ⁰⁰
*Credit + Eviction + Criminal	\$29 ⁰⁰

Phone / Fax	ILA Member Price
Criminal Only	\$22 ⁰⁰
Social Search Only	\$7 ⁰⁰
Eviction + Social Search	\$13 ⁰⁰
Eviction + Social Search + Criminal	\$29 ⁰⁰

*Credit Only	\$18 ⁰⁰
*Credit + Eviction	\$25 ⁰⁰
*Credit + Eviction + Criminal	\$32 ⁰⁰

*To access these products, additional user documentation and an onsite physical inspection is necessary.

Contemporary Information Corp.

Phone: (888) 316.4242 • Fax: (800) 677.8494 • www.cicreports.com/iowa