



# ComplyTraq

## Application for Use of Consumer Reports

### **Application**

Every field on this Application MUST be completed. If not applicable, you must write N/A. Failure to fully complete this Application in its entirety and return it along with the signed Certification (attached) will delay and/or deny your approval.

### **Company Information**

Business Name (Hereinafter "User")		Website Address(es) / URLs (if applicable)		
Street Address (Physical Address)		City	State	Zip
SSN or Federal ID Number		Year Business was Established		
Main Contact	Title	Work Phone Number		

### **Principal Information (User Owner or Officer signing below)**

Principal Name		Title	Work Phone Number	
Home Address				
City/State/Zip				
Home Phone Number	Drivers License Number		Social Security Number	

### **Business References**

Business Reference (Name/Company/Title)			Contact Number	
Street Address		City	State	Zip
Business Reference (Name/Company/Title)			Contact Number	
Street Address		City	State	Zip
Business Reference (Name/Company/Title)			Contact Number	
Street Address		City	State	Zip

### **Bank Reference**

Bank Reference (Name/Company/Title)			Contact Number	
Street Address		City	State	Zip

### **FCRA Information**

For the Purposes of the FCRA, please describe your company's business (required).
<p>Please indicate your intended use of information (check all that apply):</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Related to transaction involving credit extension, account review, account collection or bankruptcy filing with respect to subject consumer.</li> <li><input type="checkbox"/> Employment purpose (USER WILL IDENTIFY TO THE PROVIDER EACH TIME A REPORT IS REQUESTED FOR THIS PURPOSE).</li> <li><input type="checkbox"/> Insurance underwriting (USER WILL IDENTIFY TO THE PROVIDER EACH TIME A REPORT IS REQUESTED FOR THIS PURPOSE).</li> <li><input type="checkbox"/> Tenant screening.</li> <li><input type="checkbox"/> Related to a business transaction involving subject consumer. (USER WILL IDENTIFY SPECIFIC BUSINESS PURPOSE EACH TIME A REQUEST IS MADE UNDER THIS CATEGORY, AND REPORT SAME TO THE PROVIDER AT POINT OF ACCESS).</li> </ul>

**Letter of Intent**

- On Company letterhead signed by an officer, owner or authorized manager, please provide the nature of your business, the intended use for the services, anticipated monthly volume and whether your Company anticipates its access to be primarily local, regional or national.

**Bona Fide Business Verification**

Copy of Business License plus one of the following must be attached (indicate which by checking the appropriate boxes):

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Copy of Business License (must be attached if required by your state, city or county and if not required, two of the other items must be chosen and attached) | <input type="checkbox"/> Articles of Incorporation / Partnership  | <input type="checkbox"/> Corporation verification with State or Federal government                                   |
| <input type="checkbox"/> Sales tax records   | <input type="checkbox"/> State and/or Federal tax records   | <input type="checkbox"/> Professional State Issued License   |
| <input type="checkbox"/> State Tax ID Certificate (not application)  | <input type="checkbox"/> Federal ID No. form (not application)  | <input type="checkbox"/> Proof of 501 (c) (3) status (non-profit, charitable, religious or educational organization) |
|  | <input type="checkbox"/> Proof of status under FCRA § 621(b) (1, 2, 3) (Federal bank, CU, air/ground carries and those subject to the Packers and Stockyards Act of 1921) |  |

Each of the following must be attached:

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Advertising Material or Business Card | <input type="checkbox"/> Copy of Business Check | <input type="checkbox"/> Copy of Principal's Photo ID / Drivers License (only if sole proprietorship, partnership or corp. in business under 1 yr) |
| <input type="checkbox"/> Copy of Current Business Phone Bill   |   |  |

Do you lease your office space?  Yes  No If yes, you must provide the following (N/A for publicly traded companies):

Copy of current Lease (must include Lease terms, the address page, the signature page and the landlord name and contact information)

**Employment Screening Information**

If you selected Employment Screening under FCRA you must provide the following:

- List Number of Employees: \_\_\_\_\_  Private Investigator License (if applicable)

**Tenant Screening Attachment Information**

If you selected Tenant Screening under FCRA you must provide three completed rental applications and one of the other items listed:

- |  |  |   |
|--|--|---|
| <input type="checkbox"/> Three completed rental applications | <input type="checkbox"/> Document filings in Landlord/Tenant Court | <input type="checkbox"/> Verify membership in local/regional/national Apartment Association |
|--|--|---|

Please provide name of complex

Are you an individual Landlord?  Yes  No If yes, you must provide the following

- |  |  |   |
|--|--|---|
| <input type="checkbox"/> Copy of title                 | <input type="checkbox"/> Public records search of property | <input type="checkbox"/> County Assessor's office records |
| <input type="checkbox"/> Copy of property tax document | <input type="checkbox"/> Property insurance documents      |   |

**Business Operating from Residence Support Information**

Is your business operating out of a residence? (NOT Unrestricted or an Apartment)  Yes  No If yes, provide one of the following:

- |   |  |
|---|--|
| <input type="checkbox"/> Corporation verification by certificate of incorporation or framework with state or federal government | <input type="checkbox"/> Sole proprietorship/partnership verification by business license from county or state government or fictitious name application |
|---|--|

**Attorney or Law Firm Support Information**

Is Lawyer/Law Firm a) solely in collections, b) filing consumer bankruptcies or c) hiring employees?  Yes  No If yes, provide one of the following:

- |   |  |   |
|---|--|---|
| <input type="checkbox"/> Attorney State Identification Card | <input type="checkbox"/> Bar Association Membership Card | <input type="checkbox"/> Verify licensure from <a href="http://www.martindale.com">www.martindale.com</a> |
|---|--|---|

**Compliance Assurances**

Client agrees, acknowledges and warrants, as either an approved end user ("End User") or as an approved third party sales agent distributor ("Sales Agent") to End Users of various credit related products and services, ("Reports") that as applicable:

1. Sales Agents may only distribute Reports to approved End Users who have a "permissible purpose" as defined in the FCRA to request such Reports and to no other third party, and may not themselves be End Users of Reports, nor have access to or use of the Reports; and
2. It shall abide by and accept responsibility for accessing and distributing (as to Sales Agents), using and storing (as to End Users) the Reports in accordance with the Fair Credit Reporting Act, 15 U.S.C. §1681 et. seq., ("FCRA") as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") and thereafter from time to time, the Gramm-Leach-Bliley Act of 1999 ("GLB Act"), the Driver Privacy Protection Act ("DPPA"), the laws of the applicable state issuing Motor Vehicle Records ("MVR"), the Equal Credit Opportunity Act ("ECOA"), the Truth In Lending Act ("TILA") and all other applicable local, state and federal laws regarding the Reports, as well as the permissions and limitations of the credit bureaus, data repositories, ComplyTraq and other vendors providing access to the Reports, when Reports subject to such acts and laws is accessed, distributed, used and/or stored, and as applicable, adhere to the "Notice to Users of Consumer Reports: Obligations of Users Under the FCRA" and the "Notice to Furnishers of Information: Obligations of Furnishers Under the FCRA," received hereunder as required by the FCRA, and be aware that access to certain Reports is subject to restrictions of the Repository providing

such Report, such that End Users shall not export such Reports, related documentation or technical data, or any product incorporating such, outside of the fifty (50) states of the United States of America and its territories; and

3. End Users shall obtain in advance and retain on file appropriate application, release, consent and/or authorization forms (“Forms”) from any credit applicant, job applicant or other individual on whom Reports are sought; and
4. End Users shall disclose to each such individual(s) as and when required by law, that credit and/or other Reports (including investigative credit report data, if applicable) will be sought on such individual(s); and
5. End Users shall provide consumer(s) with questions about their own credit report or when credit is denied, terminated or changed or when an application is declined, based in whole or in part on such Reports, resulting in “adverse action” as defined in the FCRA, with the relevant Repository’s name, address and toll free phone number (and not that of any other Repository, vendor, partner or customer); and
6. End Users shall both advise applicants and follow procedures itself, regarding Repository mandates on inquires and complaints and retain Forms for a minimum of five (5) years in all cases where credit is extended or an application approved and in any case where credit is declined or an application declined and promptly make available such Forms to the Repositories upon reasonable notice for occasions where confirmation or audit is required by the Repositories; and
7. End Users shall take all reasonable precautions to ensure that consumer Credit Information on individuals will be held in strict confidence, disclosed only to those of its employees whose duties reasonably relate to the legitimate business purpose for which the information was requested and not disclosed to any other party in whole or in part unless required by valid subpoena, court order or applicable law; and
8. Prior to requesting each consumer report, End Users shall be identified as the end user of the consumer report, certify each “permissible purpose” as defined in the FCRA for which the consumer report will be used and that the consumer report will be used for no other purpose; and
9. Compliance and keeping up to date with new requirements or laws regarding access to or use of Reports is the responsibility of Client; and
10. End Users may secure consumer credit and other Reports on individuals solely for End Users’ own internal one-time use in accordance with the permissions and restrictions promulgated by the Repositories, which may differ from one another, which may include credit, employment, insurance underwriting, collection, government licensing or written consumer consent or initiated transactions between itself and the consumer / individual to whom information refers and/or for such other “permissible purpose” related to a business transaction as is defined by the FCRA and/or as permitted and restricted by the Repositories, and may not be resold, sub-licensed or otherwise revised in any way or delivered to any third party; and
11. As necessary, in accordance with FCRA, FACTA, GLBA, DPPA, MVR, ECOA, TILA and other local, state and federal laws, as well as Credit Bureau, Repository, ComplyTraq and other vendor policies, prior to Sales Agent distributing and End User accessing the particular desired consumer credit information, data or other Reports and on an annual basis and when changing business addresses and as new products and services are offered for access from time to time and new laws, Credit Bureau, Repository, ComplyTraq and vendor policies are established or amended, Client agrees to undergo and pay for compliance certification, credentialing, employee FCRA training and testing, an on-site inspection at its business premises (“Site Inspection”), criminal, consumer credit and other background checks on Client’s business and its principal (owner or officer), performed by ComplyTraq, to determine and review Client’s credit, history, procedures, processes and Sales Agent’s need for accessing and distributing and End User’s need for using and storing consumer credit information, data or other Reports, security practices and other protective measures in place, so as to ensure Client’s initial compliance, as well as periodically for reassurance thereafter. To ensure its End Users’ compliance, Sales Agents shall enter into a “ComplyTraq Compliance Services Agreement” directly with ComplyTraq.

The signature of Client’s authorized representative acknowledging acceptance of the above terms and conditions is set forth at the end of the attached Certification.

### **Access Security Requirements**

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. 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 minimum baselines for information security.

In accessing Experian’s services, you agree to follow 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.

#### **Data Access Security**

1. You must protect your account numbers and passwords so that only key personnel know this sensitive information. Unauthorized persons should never have knowledge of your passwords. Do not post or leave such information unattended in any manner.
2. System access software, whether developed by your company or purchased from a third party vendor, must have your account numbers and passwords “hidden” or embedded and be known only by supervisory personnel. Assign each user of your systems, a unique user ID logon and password.
3. Do not discuss your account numbers and passwords by telephone with any unknown caller, even if the caller claims to be an employee of a Credit Bureau or other data Repository.
4. Restrict the ability to obtain consumer credit and other information to only a few key End User personnel.
5. Point of sale End Users utilizing the drivers license scanning product must make consumers aware via posters and obtain written consent that drivers license data is being collected and such will be used for fraud prevention and transaction dispute resolution and will not be used for marketing.
6. Place all terminal devices used to obtain consumer credit and other information in a secure location within End User’s facility. You should secure these devices so that unauthorized persons cannot access them.
7. After normal business hours, be sure to turn off and lock all End User devices or systems used to obtain or store consumer credit and other information.
8. Secure hard copy and electronic files of consumer credit and other information within End User’s facility to prevent unauthorized access.
9. Shred or destroy all hard copy consumer credit and other information when no longer needed by End User in accordance with applicable contract, Repository regulation or law.
10. Erase or scramble End User electronic files containing consumer credit and other information when no longer needed in accordance with applicable contract, Repository regulation or law.
11. Advise all End User employees that your company can access consumer credit and other information only for the “permissible purposes” (as defined in the FCRA) identified herein and in your Agreement and that

they may not, even for testing purposes, access their own consumer credit report or that of a family member, friend, public figure or celebrity, if your company does not have permissible purpose.

**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.”*

### **Internal Systems Security**

Internal Systems that have access to sensitive consumer or other non-public personally identifiable information, including those of your customers who will have access to your system, should implement the following security measures on their systems.

1. Use of screensavers (15 minute timeout maximum) for all personnel should be mandatory.
2. User Names and password rules must be set according to the **User Name and Password Security** section herein.

### **Application Security**

When building an application system that will request, house or display sensitive consumer or other non-public personally identifiable information to an end user, the following measures must be put in place to help ensure unauthorized access of such data.

1. Technical measures to prevent screen scraping or robotic harvesting of any consumer or other non-public personally identifiable information, including information that can be viewed prior to purchasing a product, as well as contractual prohibitions on end users' right to screen scrape or robotic harvest.
2. The system should be set up so that account velocity is automatically measured and monitored for unusual activity. The system should also have the ability to turn off an individual account's access to consumer or other non-public personally identifiable information, if the account velocity threshold is tripped, and shut down access within 15 minutes if the site velocity threshold is tripped.
3. User Names and password rules must be set according to the **User Name and Password Security** section herein.
4. IP address restrictions are required for all users who will be accessing sensitive consumer or other non-public personally identifiable information. The IP address of the end user who is accessing the system must be known and set up to have such access in order to view sensitive consumer or other non-public personally identifiable information. The system must not allow users to access the system from an unknown or foreign IP address.
5. All transactions, XML and Web Based Applications must be sent over an encrypted medium. Valid encryption strategies are either HTTPS (SSL) V3 or better and at least 128 bit or HTTP over an IP Secure VPN.

### **User Name and Password Security**

The following rules must be implemented when establishing User Names and passwords:

1. User Names must be at least Eight (8) characters in length.
2. All passwords must be at least eight (8) characters in length.
3. User Names and passwords cannot be the same.
4. Passwords cannot contain the User Name.
5. All passwords must contain any two (2) of the following: alphabetic characters, numeric characters, or symbol characters.
6. All Users must have a unique User Name and password.
7. Passwords should not be written down anywhere and User Names and passwords may not be shared.
8. Users must change their passwords at a minimum of once every 90 days.
9. Users' account and access shall be suspended after five (5) unsuccessful login attempts.
10. Security administrators should be notified immediately if the User has any reason to believe their User Name or password may have been compromised.
11. Inactive Users should be suspended after 90 days.
12. All suspended Users must change their passwords upon their next login.

### **Permissible Purpose Guidelines**

Section 604 of the FCRA sets forth the “permissible purposes” (as defined therein) for companies to obtain consumer information from a credit-reporting agency:

- a. Intend to use the information in connection with a credit transaction involving the consumer on whom the information is being furnished, or
- b. Intend to use the information for employment purposes, or
- c. Intend to use the information in connection with the underwriting of insurance, or
- d. Intend to use the information in connection with a collection, or
- e. Intend to use the information in connection with a transaction initiated by the consumer, or
- f. Intend to use the information in connection with the written consent of the consumer, or
- g. Intend to use the information in connection with government licensing.

If your product lines are for different permissible purposes as listed above, a separate intended use must be identified each time for each type. If you intend to use a consumer report for employment purposes or in connection with a consumer bankruptcy filing, you must inform us of the intent and complete the appropriate documents to receive the proper inquiry coding required. If you are contacted by us or a consumer whose consumer information you have accessed, you *must* provide us or the consumer with the name and address of the person to whom the report was sold.

### **Exception List**

Notwithstanding the above, the credit bureaus and data repositories have identified certain types of companies to which consumer information cannot be sold. We have chosen to be even more restrictive and will not sell consumer information to:

- Credit or Financial Repair or Counseling (unless for non-profit, housing counseling or registered securities broker).
- Lawyers or Law Firms (unless sole practice is collections or those filing consumer bankruptcies or for employment).
- Private Investigator, Detectives or Law Enforcement (unless sole use is for employment purposes and an individual certification of permissible purpose is provided each time a report is requested).
- News Agencies or Journalists (unless sole use is for employment purposes or the review of a subscriber's credit and an individual certification of permissible purpose is provided each time a report is requested).
- Bail Bonds business or Repossession company (unless business is established, reputable or state licensed).
- Pawn Shop (unless business is reputable and in a secure and safe location).
- Process Server, Dance Studio, Check Cashing, Spiritual, Tattoo, Health, Book Club, Adult, Dating, Massage Service
- Companies: a) not in the traditional financial services industry; b) not routinely needing consumer reports in the ordinary course of business; c) providing reports direct to consumers; d) with questionable reputations or ethical natures or no legitimate need for consumer reports; e) officers or employees involved in credit fraud or other unethical business practices; or f) identified by a credit bureau or data repository as restricted.

### **FCRA Requirements**

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

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. We have included a copy of the FCRA with your membership kit. 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	Responsibility of Furnishers of Information to Consumer Reporting Agencies

Each of these sections is of direct consequence to users whom 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 initiated by the subject of the report such as tenant screening, 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 and state statutes and regulations in the locale you operate.

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

### **FACT Act Summary & Notices**

Following a public comment period, the Federal Trade Commission issued final summaries of identity theft and general consumer rights and revised furnisher and user notices under the FCRA and the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Consumer reporting agencies are required to notify consumers of their rights under FACTA and steps they can take to protect themselves against identity theft and difficulties resulting there from.

The identity theft rights summary includes the major new identity theft rights granted to consumers by FACTA, including the right to place fraud alerts on their credit reports, to block businesses and credit bureaus from reporting information in their credit files that is a result of identity theft, and to obtain from businesses information about accounts or transactions in their name that result from identity theft. The identity theft rights summary will be provided by consumer reporting companies to consumers who contact the agencies because they believe they are victims of fraud or identity theft.

The general consumer rights summary includes, among other things, consumers' right to see their credit files and know when they have been used against them, to correct inaccuracies, and to opt-out of unsolicited offers. The summary also notes that, in addition to identity theft victims, active duty military personnel have additional rights under the FCRA and FACTA. This general summary of rights updates the current summary, which credit reporting companies provide to consumers with their credit reports. The furnisher and user notices explain to businesses their duties under the FCRA.

The FTC received 50 comments from individuals, businesses, and associations. In response to these comments, the Commission has made some changes to the proposed summaries and notices it issued in July 2004, including: (1) the addition of a Spanish-language statement at the top of the summary of rights indicating where Spanish-speaking consumers may go to obtain more information in Spanish; (2) clarification that a consumer must contact the nationwide consumer reporting companies to request that a fraud alert be placed on his or her credit file, and that the initial alert remains in a consumer's file for at least 90 days; and (3) clarification that a consumer may request that a consumer reporting company block any information, not just account information, in the consumer's file if the information is the result of identity theft.

The FTC vote to approve the final rule and the publication of the Federal Register notice was 5-0.

To view the summary and notices, please click below or visit our website or contact us to request copies.

FCRA: <http://www.ftc.gov/os/statutes/031224fcra.pdf>

GLBA: <http://www.ftc.gov/privacy/glbact/glboutline.pdf>

DPPA: <http://www.nydmv.state.ny.us/forms/mv15dppa.pdf>

ADA: <http://www.sba.gov/ada/smbusgd.pdf>

Summaries of Rights and Notices of Duties Under the FCRA and FACT Act: Publication of Final Guidance on Model Disclosures: <http://www.ftc.gov/os/2004/11/041119facta.pdf>

Appendix E: Summary of Consumer Identity Theft Rights: Remediating the Effects of Identity Theft: <http://www.ftc.gov/os/2004/11/041119factaappe.pdf>

Appendix F: Summary of Consumer Rights Under the FCRA: <http://www.ftc.gov/os/2004/11/041119factaappf.pdf>

Appendix G: Notice to Furnishers of Information: Obligations of Furnishers Under the FCRA: <http://www.ftc.gov/os/2004/11/041119factaappg.pdf>

Appendix H: Notice to Users of Consumer Reports: Obligations of Users Under the FCRA: <http://www.ftc.gov/os/2004/11/041119factaapph.pdf>

### **Employment Screening Requirements**

If your business intends to use / sell credit reports and information for employment screening purposes, please read carefully.

Certain bureau products (Experian's Employment Insight, Equifax's Persona Report) may be sold to members who access credit reports and information for employment purposes. These reports differ from the consumer credit profile by suppressing information that is not applicable to an employment decision or may inadvertently violate an equal opportunity law. Suppressed information includes account numbers, year of birth and spouse references. Such bureau products also notify applicants that their file was accessed if it contains derogatory public record information,

such as bankruptcies, liens and judgments. Additionally, inquiries only display on the report provided to the applicant. They do not display on the report provided to a potential employer.

The Consumer Credit Reporting Reform Act of 1996 added to the FCRA a new section 604 (b), governing the use of consumer reports (and other data, including, but not limited to, motor vehicle, criminal and eviction data) for employment purposes. This membership packet includes the necessary documents to comply with the new law and to implement appropriate internal procedures.

Brief overview of Section 604 (b) of the amended FCRA:

The FCRA essentially mandates four conditions on credit reports for employment purposes:

1. Before pulling a credit report, the end user must provide a “clear and conspicuous” written disclosure to the consumer in a document that consists solely of the disclosure, that a consumer report may be obtained for employment purposes, and obtain a written authorization from the consumer to pull his or her credit report;
2. Before taking any adverse actions based in whole or in part on the credit report, the end user must provide the consumer a copy of the report, and a written summary of the consumer’s rights as prescribed by the FCRA;
3. The end user must certify to the credit reporting agency/reseller that in addition to complying as above, the report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation; and
4. Consumer reporting agency must provide with the credit report a Summary of Consumers Rights.

This notice is not intended to provide you with legal advice regarding the Consumer Credit Reporting Reform Act of 1996 but rather represents an interpretation of the changes mandated by the Act. Please consult your legal counsel for verification of and more detailed information regarding the Consumer Credit Reporting Reform Act of 1996.

### **Employment Compliance Certification**

In compliance with the Federal Fair Credit Reporting Act as amended by the Consumer Credit Reporting Reform Act of 1996 (the “Act”), User, as applicable, hereby certifies to Consumer Reporting Agency that it will comply with the following provisions:

1. 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 User.
2. In using a consumer report for employment purposes, before taking any adverse action based in whole or in part on the report, 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 entitled

“Summary of

Consumers Rights” can be downloaded from [www.ComplyTraq.com/ConsumerRights](http://www.ComplyTraq.com/ConsumerRights) or supplied upon request.

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

The requirements herein shall not apply if the report is provided to the employer in connection with suspected misconduct related to employment, or in compliance with federal, state or local laws and regulations, the rules of a self-regulatory organization (as defined in the Sarbanes-Oxley Act of 2002), it is not obtained for the determining the individual’s credit worthiness and it is only provided to the employer, a federal agency, a self regulatory organization or as required by law.

The signature of User’s authorized representative acknowledging acceptance of the above terms and conditions is set forth at the end of the attached Certification.

### **California Civil Code Section 1785.14(a) End User Compliance Certification**

Section 1785.14(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met:

Section 1785.14(a)(1) states: “If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver’s license number,

place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name."

Section 1785.14(a)(2) states: "If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller must certify, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail."

Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed."

In compliance with Section 1785.14(a) of the California Civil Code, by the signature of End User's authorized representative acknowledging acceptance of the above terms and conditions set forth at the end of the attached Certification, End User hereby certifies to the Consumer Reporting Agency as indicated above, whether it is or is not a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale").

End User also certifies that if it is a Retail Seller who conducts Point of Sale transactions, it will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person.

End User also certifies that it will only use the appropriate End User code number designated by the Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller.

If End User is not a Retail Seller who issues credit in Point of Sale transactions, it agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, it shall provide written notice of such to the Consumer Reporting Agency prior to using credit reports with Point of Sale transactions as a Retail Seller, and shall comply with the requirements of a Retail Seller conducting Point of Sale transactions, as provided in this certification.

#### **Vermont FCRA Compliance Certification**

End User certifies that if it orders information services relating to Vermont residents that are credit reports as defined by the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999), as amended ("VFCRA"), End User will do so only after it has received prior consumer consent in accordance with VFCRA § 2480e (set forth below), as well as the Vermont Rules (set forth below), and other applicable laws and rules.

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

##### **§ 2480e. Consumer Consent**

(a) A person shall not obtain the credit report of a consumer unless:

(1) the report is obtained in response to the order of a court having jurisdiction to issue such an order; or

(2) the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer.

(b) Credit reporting agencies shall adopt reasonable procedures to assure maximum possible compliance with subsection (a) of this section.

(c) Nothing in this section shall be construed to affect:

(1) The ability of a person who has secured the consent of the consumer pursuant to subdivision (a)(2) of this section to include in his or her request to the consumer permission to also obtain credit reports, in connection with the same transaction or extension of credit, for the purpose of reviewing the account, increasing the credit line on the account, for the purpose of taking collection action on the account, or for other legitimate purposes associated with the account; and

(2) The use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade Commission.

#### **Vermont Rules \*\*\* Current Through June 1999\*\*\*, Agency 06. Office of the Attorney General, Sub-Agency 031. Consumer Protection Division, Chapter 012. Consumer Fraud – Fair Credit Reporting, Rule CF 112 Fair Credit Reporting, CRV 06-031-012, CF 112.03 (1999), CF 112.03 Consumer Consent**

(a) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing if the consumer has made a written application or written request for credit, insurance, employment, housing or governmental benefit. If the consumer has applied for or requested credit, insurance, employment, housing or governmental benefit in a manner other than in writing, then the Client is required to obtain consumer consent pursuant to 9 V.S.A. §§

2480e and 2480g shall obtain said consent in writing or in the same manner in which the consumer made the application or request. The terms of this rule apply whether the consumer or the person required to obtain consumer consent initiates the transaction.

(b) Consumer consent required pursuant to 9 V.S.A. §§ 2480e and 2480g shall be deemed to have been obtained in writing if, after a clear and adequate written disclosure of the circumstances under which a credit report or credit reports may be obtained and the purposes for which the credit report or credit reports may be obtained, the consumer indicates his or her consent by providing his or her signature.

(c) The fact that a clear and adequate written consent form is signed by the consumer after the consumer's credit report has been obtained pursuant to some other form of consent shall not affect the validity of the earlier consent.

**Certification**

User has selected to utilize certain consumer products that are governed by the FCRA and Credit Bureau / Repository guidelines. Therefore, User must read all above sections and certify below that User is and will remain in compliance.

In whole or in part, ComplyTraq reserves the right, in its sole discretion, at any time and for any reason, with or without prior written notice, via email, fax, or regular US mail and with no liability to User, to modify, amend, change, alter, update, add to or delete from the terms and conditions contained in this Application and User's agreement for access to consumer credit and other personally identifiable information per Credit Bureau / Repository, vendor, legal, industry, ComplyTraq or other mandate and audit User's compliance therewith as well as the legal requirements applicable thereto, via on-site visits, notifications and/or document requests, with the date of receipt deemed to be the effective date of the notice.

For questions please call: 1-888-661-4352. The signed Certification, along with the fully completed Application, must be sent in their entirety to: Gold Line Credit Services, Inc., Attn: Customer Relations Dept., Fax: 866-662-6483.

By initialing next to each item to verify compliance, User certifies that:

- \_\_\_\_\_ It has read and accurately and fully completed the **Application** section
  - Complete all appropriate sections. Be sure to include principal information.
  - Include a minimum of three business references and one bank reference.
  - Read each item listed in the FCRA section and initial choice of use and permissible purpose.
  - Select and attach the chosen items listed in the Bona Fide Business Verification Section. Also attach a copy of a voided business check, a copy of photo id and advertising material or business card.
  - Tenant Screening companies must attach three completed rental applications along with one of the other items listed. If an individual landlord, provide one of the items listed along with a photo id.
  - If operating out of a residence (other than individual landlords), provide one of the items listed.
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Compliance Assurances** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Security Requirements** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Permissible Purpose Guidelines** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **FCRA Requirements** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Fact Act Summary & Notices** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Employment Screening Requirements** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Employment Compliance Certification** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Summary of Consumers Rights** section

User certifies that the terms on this and the prior pages have been read, the information is accurate and that the undersigned agrees to all of the above terms and conditions as written on behalf of User and represents that he / she is authorized to execute on behalf of User and that facsimile signatures shall be construed as valid and binding marks.

\_\_\_\_\_  
Company Name

\_\_\_\_\_  
Signature of Owner or Officer

\_\_\_\_\_  
Name Typed or Printed

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

## CREDIT SCORING SERVICES AGREEMENT

This Credit Scoring Services Agreement, ("Agreement"), dated: \_\_\_\_\_, between \_\_\_\_\_ ("End User") and Gold Line Credit Services, Inc. ("Provider")

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

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

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

### 1. General Provisions

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

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

**C. Term.** The term of this agreement will be affective as long as the end user is still a member of Gold Line Credit Services, Inc., unless otherwise terminated for non compliance.

### 2. Experian/Fair, Isaac Scores

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

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

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

**3. Fees.** There are no additional fees associated with receiving the fico score.

#### 4. Intellectual Property

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

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

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

#### 5. Compliance and Confidentiality

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

**B. Confidentiality.** End User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. End User will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, End User will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of End User and while in transport between the parties. End User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian's and Fair, Isaac's express written permission. **Proprietary Criteria.** Under no circumstances will End User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair, Isaac in performing the scoring services hereunder.

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

#### 6. Indemnification and Limitations

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

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

**7. Miscellaneous**

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

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

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

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

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

Title: \_\_\_\_\_

# GOLD LINE CREDIT SERVICES INC.

## Credit Card Charge Form

Please complete this form and mail or fax with your application.

Indicate what you would like your credit card used for:

- One time use                       Monthly billing                       Invoicing Only

**Cardholder Name (printed)** \_\_\_\_\_

**Cardholder Billing Address** \_\_\_\_\_

\_\_\_\_\_

**Card Type:**     Master Card     Visa     Discover     American Express

**Card Number** \_\_\_\_\_ **Exp Date:** \_\_\_\_\_

**CVC Number** \_\_\_\_\_ (Located on backside, next to your signature on Visa, MC & Discover cards. On front on AMX)

**Cardholder Signature** \_\_\_\_\_

I authorize my credit card to be charged for payment of the outstanding balance owed to GLC which is past due by sixty (60) days or more.

Mailing Address

Gold Line Credit Services, Inc.  
216 N. East Street  
Woodland, CA 95695

FAX Number: (866) 662-6483

Note: Fax machine is located in a secure area accessible to staff only.