All users of consumer reports must comply with all applicable regulations, including regulations promulgated after this notice was first prescribed in 2004. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

NOTICE TO USERS OF CONSUMER REPORTS:
OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Bureau of Consumer Financial Protection's website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the Bureau's website. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

- As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5)

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term "adverse action" is defined very broadly by Section 603. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA – such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained From Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active Duty Military Alerts are in Files

When a consumer has placed a fraud alert, including one relating to identify theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the the consumer's file. When this occurs, users must comply with regulations specifying the

procedures to be followed, which will be issued by the Consumer Financial Protection Bureau and the banking and credit union regulators.

The Consumer Financial Protection Bureau regulations will be available at www.consumerfinance.gov/learnmore/.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. The Consumer Financial Protection Bureau, the Securities and Exchange Commission, and the banking and credit union regulators have issued regulations covering disposal. The Consumer Financial Protection Bureau regulations may be found at www.consumerfinance.gov/learnmore/.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations prescribed by the Consumer Financial Protection Bureau.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) (“Notice to the Home Loan Applicant”).

III. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

If the information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer’s rights will be provided to the consumer.
- **Before** taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer’s rights (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2).

The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.
- Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in regulations issued by the banking and credit union regulators) – the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or a permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(1), 604(c), 604(e), and 614(d). This practice is known as "prescreening" and typically involves obtaining a list of consumers from a CRA who meet certain preestablished criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.

- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, the Consumer Financial Protection Bureau has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The relevant regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
  1. the identity of all end-users;
  2. certifications from all users of each purpose for which reports will be used; and
  3. certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

The Consumer Financial Protection Bureau website, www.consumerfinance.gov/learnmore, has more information about the FCRA.

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1618 et seq.:

Section 602	15 U.S.C. 1681
Section 603	15 U.S.C. 1681a
Section 604	15 U.S.C. 1681b
Section 605	15 U.S.C. 1681c
Section 605A	15 U.S.C. 1681cA
Section 605B	15 U.S.C. 1681cB
Section 606	15 U.S.C. 1681d
Section 607	15 U.S.C. 1681e
Section 608	15 U.S.C. 1681f
Section 609	15 U.S.C. 1681g
Section 610	15 U.S.C. 1681h
Section 611	15 U.S.C. 1681i
Section 612	15 U.S.C. 1681j
Section 613	15 U.S.C. 1681k
Section 614	15 U.S.C. 1681l
Section 615	15 U.S.C. 1681m
Section 616	15 U.S.C. 1681n
Section 617	15 U.S.C. 1681o
Section 618	15 U.S.C. 1681p
Section 619	15 U.S.C. 1681q
Section 620	15 U.S.C. 1681r
Section 621	15 U.S.C. 1681s
Section 622	15 U.S.C. 1681s-1
Section 623	15 U.S.C. 1681s-2
Section 624	15 U.S.C. 1681t
Section 625	15 U.S.C. 1681u
Section 626	15 U.S.C. 1681v
Section 627	15 U.S.C. 1681w
Section 628	15 U.S.C. 1681x
Section 629	15 U.S.C. 1681y

Birchwood
CREDIT SERVICES, INC.

Access Security Requirements for Reseller End-Users

for FCRA and GLB 5A Data

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

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

1. Implement Strong Access Control Measures

1.1 All credentials such as User names/identifiers/account numbers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Birchwood Credit Services Inc. will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Birchwood's systems, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing Birchwood Credit Services Inc. data/ systems.

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

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

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

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

1.7 Develop strong passwords that are:

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

1.8 Passwords (e.g. user/account password) must be changed immediately when:

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

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

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

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

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

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

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

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

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

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

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

2. **Maintain a Vulnerability Management Program**

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

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

2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

3. **Protect Data**

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

3.2 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such as AES 256 or above.

3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

4. Maintain an Information Security Policy

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

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.

4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe Experian data may have been compromised, immediately notify Birchwood Credit Services Inc. within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with the Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian's list of compliant service providers. If the service provider is in the process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. Approved certifications in lieu of EI3PA can be found in the Glossary section.

5. Build and Maintain a Secure Network

5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand-alone computers that directly access the Internet must have a desktop firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

5.5 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access Birchwood Credit Services Inc. systems, access to third party tools/services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Birchwood Credit Services Inc. systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

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

7. Mobile and Cloud Technology

7.1 Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian in writing; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

7.3 Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

7.4 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Experian data via mobile applications (internally developed or using a third party application),

ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

7.7 When using cloud providers to access, transmit, store, or process Experian data ensure that:

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
  - ISO 27001
  - PCI DSS
  - EI3PA
  - SSAE 16 – SOC 2 or SOC3
  - FISMA
  - CAI / CCM assessment

8. General

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

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to Birchwood Credit Services Inc. upon request, audit trail information and management reports generated by the vendor software, regarding Company individual authorized users.

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

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

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

8.5 Reasonable access to audit trail reports of systems utilized to access Birchwood Credit Services Inc. systems shall be made available to Birchwood Credit Services Inc. upon request, for example during breach investigation or while performing audits.

8.6 Data requests from Company to Birchwood Credit Services Inc. must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Experian to Birchwood Credit Services Inc. within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Birchwood Credit Services Inc. of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under

and in compliance with applicable law. Telephone notification is preferred at 800-910-0015, Email notification will be sent to info@birchwoodcreditservices.com

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Birchwood Credit Services Inc. services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.

8.9 Company understands that its use of Birchwood Credit Services Inc. networking and computing resources may be monitored and audited by Birchwood Credit Services Inc. without further notice.

8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/ authorized users, and for assuring that mechanisms to access Birchwood Credit Service Inc. services or data are secure and in compliance with its membership agreement.

8.11 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by Birchwood Credit Services Inc.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Experian requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.

"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

Internet Delivery Security Requirements

In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Birchwood Credit Services, Inc. provided services via Internet ("Internet Access").

General requirements:

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Birchwood Credit Services, Inc. on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Birchwood Credit Services, Inc. provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.

2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Birchwood Credit Services, Inc. product based upon the legitimate business needs of each employee. Birchwood Credit Services, Inc. shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.

3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Birchwood Credit Services, Inc. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). Birchwood's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Birchwood Credit

Services, Inc. may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. Note: Partially completed forms and verbal requests will not be accepted.

4. An officer of the Company agrees to notify Birchwood Credit Services, Inc. in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Birchwood Credit Services, Inc. on systems access related matters. This individual be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Birchwood Credit Services, Inc. on information and product access, in accordance with these Experian Access Security Requirements for Reseller End-Users. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Birchwood's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Birchwood Credit Services, Inc. immediately.

2. As a Client to Birchwood's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.

3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Birchwood Credit Services, Inc. product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Birchwood's Security Administration group on information and product access matters.

4. The Head Designate shall be responsible for notifying their corresponding Birchwood Credit Services, Inc. representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.

2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).

3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.

4. Is responsible for ensuring that Company's Authorized Users are authorized to access Birchwood Credit Services, Inc. products and services.

5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.

6. Must immediately report any suspicious or questionable activity to Birchwood Credit Services, Inc. regarding access to Birchwood's products and services.

7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Birchwood Credit Services, Inc.

8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.

9. Shall be available to interact with Birchwood Credit Services, Inc. when needed on any system or user related matters.

Glossary

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

ISO 27001 /27002	ISO 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Birchwood
CREDIT SERVICES, INC.

ADDENDUM A-1

Qualified Subscriber Terms and Conditions

Equifax Information Services LLC ("Equifax")

Equifax Information Services (as defined below) will be received by Qualified Subscriber through CRA subject to the following conditions (the "Terms and Conditions"):

1. Any information services and data originating from Equifax (the "Equifax Information Services" or "Equifax Information") will be requested only for Subscriber's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted under the last sentence of this Paragraph. Only designated representatives of Qualified Subscriber will request Equifax Information Services on Qualified Subscriber's employees, and employees are forbidden to obtain consumer reports on themselves, associates or any other persons except in the exercise of their official duties. Qualified Subscriber will not disclose Equifax Information to the subject of the report except as permitted or required by law, but will refer the subject to Equifax.

2. Qualified Subscriber will hold Equifax and all its agents harmless on account of any expense or damage arising or resulting from the publishing or other disclosure of Equifax Information by Qualified Subscriber, its employees or agents contrary to the conditions of Paragraph 1 or applicable law.

3. Recognizing that information for the Equifax Information Services is secured by and through fallible human sources and that, for the fee charged, Equifax cannot be an insurer of the accuracy of the Equifax Information Services, Qualified Subscriber understands that the accuracy of any Equifax Information Service received by Qualified Subscriber is not guaranteed by Equifax, and Qualified Subscriber releases Equifax and its affiliate companies, affiliated credit bureaus, agents, employees, and independent contractors from liability, even if caused by negligence, in connection with the Equifax Information Services and from any loss or expense suffered by Qualified Subscriber resulting directly or indirectly from Equifax Information.

4. Qualified Subscriber will be charged for the Equifax Information Services by CRA, which is responsible for paying Equifax for the Equifax Information Services.

5. Written notice by either party to the other will terminate these Terms and Conditions effective ten (10) days after the date of that notice, but the obligations and agreements set forth in Paragraphs 1, 2, 3, 6, 7, and 8 herein will remain in force.

6. Qualified Subscriber certifies that it will order Equifax Information Services that are consumer reports, as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FCRA"), only when Qualified Subscriber intends to use that consumer report information: (a) in accordance with the FCRA and all state law counterparts; and (b) for one of the following permissible purposes: (i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; (ii) in connection with the underwriting of insurance involving the consumer; (iii) as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; (iv) when Qualified Subscriber otherwise has a legitimate business need for the information either in connection with a business transaction that is initiated by the consumer, or to review an account to determine whether the consumer continues to meet the terms of the accounts; or (v) for employment purposes; provided, however, that QUALIFIED SUBSCRIBER IS NOT AUTHORIZED TO REQUEST OR RECEIVE CONSUMER REPORTS FOR EMPLOYMENT PURPOSES UNLESS QUALIFIED SUBSCRIBER HAS AGREED IN WRITING TO THE TERMS AND CONDITIONS OF THE EQUIFAX PERSONA SERVICE. Qualified Subscriber will comply with the applicable provisions of the FCRA, Federal Equal Credit Opportunity Act, GrammLeach-Bliley Act and any amendments to them, all state law counterparts of them, and all applicable regulations promulgated under any of them including, without limitation, any provisions requiring adverse action notification to the consumer. Qualified Subscriber will use each consumer report ordered under these Terms and Conditions for one of the foregoing purposes and for no other purpose.

7. It is recognized and understood that the FCRA provides that anyone "who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two (2) years, or both." Equifax may periodically conduct audits of Qualified Subscriber regarding its compliance with these Terms and Conditions, including, without limitation, the FCRA, other certifications and security provisions in these Terms and Conditions. Audits will be conducted by mail whenever possible and will require Qualified Subscriber to provide documentation as to permissible use of particular consumer reports. Qualified Subscriber gives its consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Qualified Subscriber's material breach of these Terms and Conditions, constitute grounds for immediate suspension of service or termination of these Terms and Conditions, notwithstanding Paragraph 5 above. If Equifax terminates these Terms and Conditions due to the conditions in the preceding sentence, Qualified Subscriber (i) unconditionally releases and agrees to hold Equifax harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and (ii) covenants it will not assert any claim or cause of action of any kind or nature against Equifax in connection with such termination.

8. California Law Certification. Qualified Subscriber will make the following certification,and Qualified Subscriber agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act.

(PLEASE CHECK ("X") THE APPROPRIATE LINE BELOW)

Qualified Subscriber certifies that it ____ IS or ____IS NOT a "retail seller," as defined in Section 1802.3 of the California Civil Code and ____ DOES or ____ DOES NOT issue credit to consumers who appear in person on the basis of an application for credit submitted in person.

9. Vermont Certification. Qualified Subscriber certifies that it will comply with applicable provisions under Vermont law. In particular, Qualified Subscriber certifies that it will order information services relating to Vermont residents that are credit reports as defined by the Vermont Fair Credit Reporting Act ("VFCRA"), only after Qualified Subscriber has received prior consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Qualified Subscriber further certifies that the attached copy of Section 2480e (Exhibit 1-B) of the Vermont Fair Credit Reporting Statute was received.

10. Data Security.

    10.1. This Paragraph 10 applies to any means through which Qualified Subscriber orders or accesses the Equifax Information Services including, without limitation, system-to-system, personal computer or the Internet; provided, however, if Qualified Subscriber orders or accesses the Equifax Information Services via the Internet, Qualified Subscriber shall fully comply with Equifax's connectivity security requirements specified in Paragraph 10.3, below.

    For the purposes of this Paragraph 10, the term "Authorized User" means a Qualified Subscriber employee that Qualified Subscriber has authorized to order or access the Equifax Information Services and who is trained on Qualified Subscriber's obligations under these Terms and Conditions with respect to the ordering and use of the Equifax Information Services, and the information provided through same, including Qualified Subscriber's FCRA and other obligations with respect to the access and use of consumer reports.

    10.2. Qualified Subscriber will, with respect to handling Equifax Information:

    (a) ensure that only Authorized Users can order or have access to the Equifax Information Services,

    (b) ensure that Authorized Users do not order credit reports for personal reasons or provide them to any third party except as permitted by these Terms and Conditions,

(c) ensure that all devices used by Qualified Subscriber to order or access the Equifax Information Services are placed in a secure location and accessible only by Authorized Users, and that such devices are secured when not in use through such means as screen locks, shutting power controls off, or other commercially reasonable security procedures,

(d) take all necessary measures to prevent unauthorized ordering of or access to the Equifax Information Services by any person other than an Authorized User for permissible purposes, including, without limitation, limiting the knowledge of the Qualified Subscriber security codes, member numbers, User IDs, and any passwords Qualified Subscriber may use, to those individuals with a need to know, changing Qualified Subscriber's user passwords at least every ninety (90) days, or sooner if an Authorized User is no longer responsible for accessing the Equifax Information Services, or if Qualified Subscriber suspects an unauthorized person has learned the password, and using all security features in the software and hardware Qualified Subscriber uses to order or access the Equifax Information Services,
(e) in no event access the Equifax Information Services via any wireless communication device, including but not limited to, web enabled cell phones, interactive wireless pagers, personal digital assistants (PDAs), mobile data terminals and portable data terminals,

(f) not use personal computer hard drives or portable and/or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs, DVDs, software, and code) to store the Equifax Information Services. In addition, Equifax Information must be encrypted when not in use and all printed Equifax Information must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose,

(g) if Qualified Subscriber sends, transfers or ships any Equifax Information, encrypt the Equifax Information using the following minimum standards, which standards may be modified from time to time by Equifax: Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms,

(h) monitor compliance with the obligations of this Paragraph 10, and immediately notify Equifax if Qualified Subscriber suspects or knows of any unauthorized access or attempt to access the Equifax Information Services. Such monitoring will include, without limitation, a review of each CRA invoice for the purpose of detecting any unauthorized activity.

(i) not ship hardware or software between Qualified Subscriber's locations or to third parties without deleting all Equifax Qualified Subscriber number(s), security codes, User IDs, passwords, Qualified Subscriber user passwords, and any consumer information,

(j) access, use and store the Information Services (for purposes of this Paragraph 10 "Information Services" shall include without limitation all information and data provided or obtained through use of the Information Services) only at or from locations within the territorial boundaries of the United States, United States territories and Canada (the "Permitted Territory"). Qualified Subscriber may not access, use or store the Information Services at or from, or send the Information Services to, any location outside of the Permitted Territory without first obtaining Equifax's written permission,

(k) inform Authorized Users that unauthorized access to consumer reports may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment, and

(l) use commercially reasonable efforts to assure data security when disposing of any consumer report information or record obtained from Equifax. Such efforts must include the use of those procedures issued by the federal regulatory agency charged with oversight of Qualified Subscriber's activities (e.g. the Federal Trade Commission, the applicable banking or credit union regulator) applicable to the disposal of consumer report information or records.

10.3. Qualified Subscriber will, with respect to Qualified Subscriber's network security:

(a) use commercially reasonable efforts to protect Equifax Information when stored on servers,

subject to the following requirements: (i) Equifax Information must be protected by multiple layers of network security, including but not limited to, firewalls, routers, and intrusion detection devices; (ii) secure access (both physical and network) to systems storing Equifax Information, must include authentication and passwords that are changed at least every 90 days; and (iii) all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available,

(b) use commercially reasonable efforts to protect Qualified Subscriber's connection with dedicated, industry-recognized firewalls that are configured and managed to adhere to industry accepted best practices,

(c) only hold Equifax Information on an application server which can only be accessed by a presentation server, through one of the following: (i) Dual or multiple firewall method (preferred) – this method consists of a firewall between the Internet and the presentation server(s) and another firewall between the presentation server(s) and the application server holding Equifax Information. The network firewall should ensure that only the presentation server(s) is/are allowed to access the application server holding Equifax Information, (ii) Single firewall method (acceptable) – when a dual firewall method is not feasible, a single firewall will provide acceptable levels of protection. The firewall should be installed between the Internet and the presentation server(s). Multiple interfaces to separate the presentation server(s) and the application server holding Equifax Information are required. The firewall should be configured to allow only the presentation server(s) access to the application server holding Equifax Information, or (iii) ensure that all administrative and network access to the firewalls and servers must be through an internal network or protected extranet using strong authentication encryption such as VPN and SSH.

(d) use commercially reasonable efforts to route communications from Qualified Subscriber's internal services to external systems through firewalls configured for network address translation (NAT).

(e) use commercially reasonable efforts to establish procedures and logging mechanisms for systems and networks that will allow tracking and analysis in the event there is a compromise, and maintain an audit trail history for at least three (3) months for review by Equifax.

10.4. If Equifax reasonably believes that Qualified Subscriber has violated this Paragraph 10, Equifax may, in addition to any other remedy authorized by these Terms and Conditions, with reasonable advance written notice to Qualified Subscriber and at Equifax's sole expense, conduct, or have a third party conduct on its behalf, an audit of Qualified Subscriber's network security systems, facilities, practices and procedures to the extent Equifax reasonably deems necessary, including an on-site inspection, to evaluate Qualified Subscriber's compliance with the data security requirements of this Paragraph 10.

11. These Terms and Conditions will be governed by and construed in accordance with the laws of the State of Georgia, without giving effect to its conflicts of laws provisions. These Terms and Conditions constitute the entire agreement of the parties with respect to Qualified Subscriber receiving Equifax Information Services and no changes in these Terms and Conditions may be made except in writing by an officer of Equifax.

Exhibit 1-B

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

§ 2480e. Consumer consent

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

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

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

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

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

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

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

VERMONT RULES * CURRENT THROUGH JUNE 1999 ***
AGENCY 06. OFFICE OF THE ATTORNEY GENERAL
SUB-AGENCY 031. CONSUMER PROTECTION DIVISION
CHAPTER 012. Consumer Fraud--Fair Credit Reporting
RULE CF 112 FAIR CREDIT REPORTING
CVR 06-031-012, CF 112.03 (1999)
CF 112.03 CONSUMER CONSENT**

(a) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and2480g shall obtain said consent in writing if the consumer has made a written application or written request for credit, insurance, employment, housing or governmental benefit. If the consumer has applied for or requested credit, insurance, employment, housing or governmental benefit in a manner other than in writing, then the person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing or in the same manner in which the consumer made the application or request.The terms of this rule apply whether the consumer or the person required to obtain consumer consent initiates the transaction.

(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.

ADDENDUM A-2

Additional Equifax Information Services

This Addendum supplements the Qualified Subscriber Terms and Conditions under which Qualified Subscriber receives, as part of its service from CRA, consumer credit report information available from Equifax Information Services LLC ("EIS" or "Equifax").

This Addendum contains additional information services available from EIS, described below, that may be provided to Qualified Subscriber subject to the Qualified Subscriber Terms and Conditions, and additional terms and conditions that apply to such additional information services. Qualified Subscriber's authorized representative must place his or her initials by each service listed below that Qualified Subscriber desires to receive. Qualified Subscriber agrees to abide by the additional terms and conditions that apply to the service(s) so selected.

_____ Auto-DTEC

_____ Bankruptcy Navigator Index 3.0

_____ BEACON

_____ Consumer Telephone Service

_____ Full DTEC

_____ North American Link

_____ OFAC Alert™

_____ On-Line Directory

_____ PERSONA

_____ Pinnacle℠

_____ Safescan

_____ VantageScore

1. **Auto-DTEC** – is a service that automatically uses the Social Security number from an original ACROFILE, ACROFILE Plus, ACRO Select or FINDERS inquiry to generate another search using a DTEC™ transaction to return a name, address and Social Security number whenever the credit file inquiry returns a "No Record Found" message.

2. **Bankruptcy Navigator Index 3.0** - is a credit scoring service that rank-orders and segments accounts according to the likelihood of bankruptcy over a 24-month period, based on information in the Equifax consumer credit database. The scores returned by the Bankruptcy Navigator Index 3.0 service only represent a prediction of bankruptcy filing relative to other individuals in the Equifax credit database and are not intended to characterize any individual as to credit risk or credit capacity. Qualified Subscriber certifies that it will order this Service only when Qualified Subscriber intends to use the information for the permissible purposes set forth in Section 604(a) of the Fair Credit Reporting Act. Qualified Subscriber will not order the Service for employment purposes.

3. **BEACON℠** - is a consumer report credit scoring service based on a model developed by Fair, Isaac and Equifax that ranks consumers in the Equifax consumer credit database relative to other consumers in the database with respect to the likelihood of those consumers paying their accounts as agreed ("Score").

4. **Consumer Telephone Number Service** – is an optional feature which allows published consumer telephone numbers to be displayed on the consumer report.

5. **Full DTEC** - is a consumer report that consists of name, AKA, or former name, current and former addresses, listed telephone number (if available), age, employment, Social Security number and a message pertaining to the Social Security number. Qualified Subscriber certifies that it will order a Full DTEC Report only when it has a permissible purpose to receive a consumer report, as specified in the Qualified Subscriber Terms and Conditions.

6. **North American Link**

   (a) Desiring to obtain credit reporting services on residents of the United States and Canada through EIS's North American Link access mechanism, Qualified Subscriber understands that credit reporting services on residents of Canada will be provided from the credit reporting database of Equifax Canada Inc. Qualified Subscriber further understands that EIS is merely facilitating access and receipt of credit reporting services from Equifax Canada Inc. and that EIS has not prepared and is not responsible for the credit reporting services received from Equifax Canada Inc.

   (b) Further, Qualified Subscriber will comply with applicable provincial laws on consumer credit reporting or on protection of personal information (privacy), including obtaining consent if required, in connection with credit reporting services received from Equifax Canada.

7. **OFAC Alert** - is an information service Equifax provides on behalf of Compliance Data Center, Inc., an Equifax affiliate. OFAC Alert is based on information that was not collected, in whole or in part, for the purpose of serving as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; employment purposes, or any other purpose authorized under the FCRA. Accordingly, Qualified Subscriber will not use an OFAC Alert indicator as part of its decision-making process for determining the consumer's eligibility for any credit or any other FCRA permissible purpose. Qualified Subscriber acknowledges that such an indicator is merely a message that the consumer may be listed on one or more U.S. government-maintained lists of persons subject to economic sanctions, and Qualified Subscriber should contact the appropriate government agency for confirmation and instructions. The OFAC Alert indicator may or may not pertain to the individual referenced in your inquiry. Refer to the OFAC Customer Guide for further information.

8. **On-line Directory** - is an ancillary service to ACROFILE→, ACROFILE Plus™, and PERSONA® that automatically provides creditors' and inquirers' names and current phone numbers on the consumer report.

9. **PERSONA®** and **PERSONA PLUS®** - are consumer reports, from the Equifax consumer credit database, consisting of limited identification information, credit file inquiries, public record information, credit account trade lines, and employment information.

   FCRA Certification. Qualified Subscriber will notify Equifax whenever a consumer report will be used for employment purposes. Qualified Subscriber certifies that, before ordering each consumer report to be used in connection with employment purposes, it will clearly and conspicuously disclose to the subject consumer, in a written document consisting solely of the disclosure, that Qualified Subscriber may obtain a consumer report for employment purposes, and will also obtain the consumer's written authorization to obtain or procure a consumer report relating to that consumer. Qualified Subscriber further certifies that it will not take adverse action against the consumer based in whole or in part upon the consumer report without first providing to the consumer to whom the consumer report relates a copy of the consumer report and a written description of the consumer's rights as prescribed by the Federal Trade Commission ("FTC") under Section 609(c)(3) of the FCRA, and will also not use any information from the consumer report in violation of any applicable federal or state equal employment opportunity law or regulation. Qualified Subscriber acknowledges that it has received from Equifax a copy of the written disclosure form prescribed by the FTC.

10. **Pinnacle℠** – is a credit scoring algorithm developed by Fair, Isaac and Equifax that evaluates the likelihood that consumers will pay their existing and future credit obligations, as agreed, based on the computerized consumer credit information in the Equifax consumer reporting database.

11. **SAFESCAN®** - is an on-line warning system containing information that can be used to detect possible fraudulent applications for credit. Some of the information in the SAFESCAN database is provided by credit grantors. SAFESCAN is a registered trademark of Equifax.

    Permitted Use. SAFESCAN is not based on information in Equifax's consumer reporting database and

is not intended to be used as a consumer report. Qualified Subscriber will not use a SAFESCAN alert or warning message in its decision-making process for denying credit or any other FCRA permissible purpose, but will use the message as an indication that the consumer's application information should be independently verified prior to a credit or other decision. Qualified Subscriber understands that the information supplied by SAFESCAN may or may not apply to the consumer about whom Qualified Subscriber has inquired.

12. **VantageScore℠** - is a tri-bureau credit risk model developed using one algorithm across sample data common to all three credit bureaus. The following additional terms and conditions apply to Qualified Subscriber's receipt and use of VantageScore:

    End User Terms for VantageScore – Qualified Subscriber will request VantageScores only for Qualified Subscriber's exclusive use. Qualified Subscriber may store VantageScores solely for Qualified Subscriber's own use in furtherance of Qualified Subscriber's original purpose for obtaining the VantageScores. Qualified Subscriber shall not use the VantageScores for model development or model calibration and shall not reverse engineer the VantageScore. All VantageScores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any person except (i) to those employees of Qualified Subscriber with a need to know and in the course of their employment; (ii) to those third party processing agents of Qualified Subscriber who have executed an agreement that limits the use of the VantageScores by the third party only to the use permitted to Qualified Subscriber and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the VantageScore; or (iv) as required by law.

Additional Terms and Conditions for Credit Score Information Applicable to Bankruptcy Navigator Index 3.0 and VantageScore:

(a) Disclosure of Scores. Qualified Subscriber will hold all information received from Equifax in connection with any Score received from Equifax under this Agreement in strict confidence and will not disclose that information to the consumer or to others except in accord with the following sentence or as required or permitted by law. Qualified Subscriber may provide the principal factors contributing to the Score to the subject of the report when those principal factors are the basis of Qualified Subscriber's adverse action against the subject consumer. Qualified Subscriber must describe the principal factors in a manner which complies with Regulation B of the ECOA.

(b) ECOA Statements. Equifax reasonably believes that, subject to validation by Qualified Subscriber on its own records, (1) the scoring algorithms used in the computation of the Score are empirically derived from consumer credit information from Equifax's consumer credit reporting database, and are demonstrably and statistically sound methods of rank ordering candidate records from the Equifax consumer credit database for the purposes for which the Score was designed particularly, and it is intended to be an "empirically derived, demonstrably and statistically sound credit scoring system" as defined in Regulation B, with the understanding that the term "empirically derived, demonstrably and statistically sound," is defined only in a general manner by Regulation B, and has not been the subject of any significant interpretation; and (2) the scoring algorithms comprising the Score, except as permitted, do not use a "prohibited basis," as such phrase is defined in Regulation B. Qualified Subscriber must validate the Score on its own records. Qualified Subscriber will be responsible for meeting its requirements under the ECOA and Regulation B.

(c) Release. Equifax does not guarantee the predictive value of the Score with respect to any individual, and does not intend to characterize any individual as to credit capability. Neither Equifax nor its directors, officers, employees, agents, subsidiary and affiliated companies, or any third-party contractors, licensors or suppliers of Equifax will be liable to Qualified Subscriber for any damages, losses, costs or expenses incurred by Qualified Subscriber resulting from any failure of a Score to accurately predict the credit worthiness of Qualified Subscriber's applicants or customers. In the event the Score is not correctly applied by Equifax to any credit file, Equifax's sole responsibility will be to reprocess the credit file through the Score at no additional charge.

(d) Audit of Models. Qualified Subscriber may audit a sample of the Scores and principal factors and compare them to the anonymous underlying credit reports in accordance with Equifax's audit procedures. If the Scores and principal reasons are not substantiated by the credit files provided for the audit, Equifax will review programming of the model and make corrections as necessary until the Scores and principal reasons are substantiated by the audit sample credit reports. After that review and approval, Qualified Subscriber will be

deemed to have accepted the resulting Score and principal factors delivered. It is Qualified Subscriber's sole responsibility to validate all scoring models on its own records and performance.

Additional Terms and Conditions for Credit Score Information Applicable to Beacon and Pinnacle:

(a) Confidentiality. Qualified Subscriber will hold all Scores received from Equifax under this Agreement in strict confidence and will not disclose any Score to the consumer or to others except as required or permitted by law. Qualified Subscriber may provide the principal factors contributing to the Score to the subject of the report when those principal factors are the basis of Qualified Subscriber's adverse action against the subject consumer. Qualified Subscriber must describe the principal factors in a manner which complies with Regulation B of the ECOA. Further, Qualified Subscriber acknowledges that the Score and factors are proprietary and that, except for (a) disclosure to the subject consumer if Qualified Subscriber has taken adverse action against such consumer based in whole or in part on the consumer report with which the Score was delivered or (b) as required by law, Qualified Subscriber will not provide the Score to any other party without Equifax's and Fair, Isaac's prior written consent.

(b) Limited Liability. The combined liability of Equifax and Fair, Isaac arising from any particular Score provided by Equifax and Fair, Isaac shall be limited to the aggregate amount of money received by Equifax from Qualified Subscriber with respect to that particular Score during the preceding twelve (12) months prior to the date of the event that gave rise to the cause of action.

(c) Adverse Action. Qualified Subscriber shall not use a Score as the basis for an "Adverse Action" as defined by the Equal Credit Opportunity Action or Regulation B, unless score factor codes have been delivered to Qualified Subscriber along with the Score.

Birchwood
CREDIT SERVICES, INC.

Addendum B

Experian Requirements

End User, in order to receive consumer credit information from Experian Information Solutions, Inc., ("Experian") via Birchwood Credit Services, Inc. ("BCS"), agrees to comply with the following conditions required by Experian, which may be in addition to those outlined in the BCS Service Agreement ("Agreement"), of which these conditions are made a part. End User understands and agrees that Experian's delivery of information to End User via BCS is specifically conditioned upon End User's agreement with the provisions set forth herein. End User understands and agrees that these requirements pertain to all of its employees, managers and owners and that all persons having access to Experian credit information, whether existing or future employees, will be trained to understand and comply with these obligations.

1. End User hereby agrees to comply with all current and future policies and procedures required by Experian and instituted by BCS. BCS will give End User as much notice as possible prior to the effective date of any such new policies that may be required in the future, but does not guarantee that reasonable notice will be possible. End User may terminate this agreement at any time after notification of a change in policy in the event End User deems such compliance as not within its best interest.

2. End User certifies that it is not involved in any business activity listed in Exhibit A to the BCS service agreement.

3. End User agrees that Experian shall have the right to audit records of End User that are relevant to the provision of services set forth in this Agreement and to verify, through audit or otherwise, that End User is in compliance with applicable law and the provisions of this Agreement. End User warrants that it is the end user of the Experian credit information with no intention to resell or otherwise provide or transfer the credit information in whole or in part to any other person or entity. End User authorizes BCS to provide to Experian, upon Experian's request, all materials and information relating to its investigations of End User. End User further agrees that it will respond within the requested time frame indicated for information requested by Experian regarding Experian consumer credit information. End User understands that Experian may require BCS to suspend or terminate access to Experian information in the event End User does not cooperate with any such an investigation, or in the event End User is not in compliance with applicable law or this Agreement. End User shall remain responsible for the payment for any services provided to End User by BCS prior to any such discontinuance.

4. End User agrees that it will maintain proper access security procedures consistent with industry standards and that if a data breach occurs or is suspected to have occurred in which Experian information is compromised or is potentially compromised, End User will take the following action:

    a. End User will notify BCS within 24 hours of a discovery of a breach of the security of consumer reporting data if the personal information of consumers was, or is reasonably believed to have been, acquired by an unauthorized person. Further, End User will cooperate with and participate in any investigation conducted by BCS or Experian that results from End User's breach of Experian consumer credit information.

    b. In the event that Experian determines that the breach was within the control of End User, End User will provide notification to affected consumers that their personally sensitive information has been or may have been compromised. Experian will have control over the nature and timing of the consumer correspondence related to the breach when Experian information is involved.

    c. In such event, End User will provide to each affected or potentially affected consumer, credit history monitoring services for a minimum of one (1) year, in which the consumer's credit history is monitored and the consumer receives daily notification of changes that may indicate fraud or ID theft, from at least one (1) national consumer credit reporting bureau.

d. End User understands and agrees that if the root cause of the breach is determined by Experian to be under the control of the End User (i.e., employee fraud, misconduct or abuse; access by an unqualified or improperly qualified user; improperly secured website, etc.), End User may be assessed an expense recovery fee.

5. End User understands that if a change of control or ownership should occur, the new owner of the End User business must be re-credentialed as a permissible and authorized End User of Experian products and services. A third party physical inspection at the new address will be required if End User changes location.

6. For the purpose of this section “authorized residential End User” shall mean that the End User office meets the physical requirements outline by Experian for a residential office.

If End User is an authorized residential End User the following additional requirements and documentation must be supplied: (a) Experian must be notified for tracking and monitoring purposes; (b) End User must maintain a separate business phone line listed in the name of the business; (c) a separate subscriber code for End User must be maintained for compliance monitoring; and (d) an annual physical inspection of the office is required by Experian, for which a reasonable fee may be required.

7. End User agrees to hold harmless Experian and its agents from and against any and all liabilities, damages, losses, claims, costs and expenses, including reasonable attorney’s fees, which may be asserted against or incurred by Experian, arising out of or resulting from the use, disclosure, sale or transfer of the consumer credit information by End User, or End User’s breach of this Agreement. End User further understands and agrees that the accuracy of any consumer credit information is not guaranteed by Experian and releases Experian and its agents from liability for any loss, cost, expense or damage, including attorney’s fees, suffered by End User resulting directly or indirectly from its use of consumer credit information from Experian.

8. Experian will not, for the fee charged for credit information, be an insurer or guarantor of the accuracy or reliability of the information. EXPERIAN DOES NOT GUARANTEE OR WARRANT THE ACCURACY, TIMELINESS, COMPLETENESS, CURRENTNESS, MECHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE INFORMATION AND SHALL NOT BE LIABLE TO END USER FOR ANY LOSS OR INJURY ARISING OUT OF OR CAUSED IN WHOLE OR IN PART BY EXPERIAN’S ACTS OR OMISSIONS, WHETHER NEGLIGENT OR OTHERWISE, IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE INFORMATION.

Birchwood
CREDIT SERVICES, INC.

Addendum B-1

Death Master File

In the event Customer orders information obtained from the Death Master File issued by the Social Security Administration, Customer certifies the following:

End User certifies that it meets the qualifications of a Certified Person under 15 CFR Part 1110.2 and that its access to the DMF is appropriate because:

a. Certified Person: End User has a legitimate fraud prevention interest, or has a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty, and shall specify the basis for so certifying; and

b. Security: End User has systems, facilities, and procedures in place to safeguard the accessed information; experience in maintaining the confidentiality, security, and appropriate use of the accessed information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986; and agrees to satisfy the requirements of such section 6103(p)(4) as if such section applied to End User; and

c. End User shall not disclose information derived from the DMF to the consumer or any third party, unless clearly required by law.

d. Penalties: End User acknowledges that failure to comply with the provisions above may subject Reseller to penalties under 15 CFR 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year.

e. Indemnification and Hold Harmless: End User shall indemnify and hold harmless the credit reporting vendors and the U.S. Government/NTIS from all claims, demands, damages, expenses, and losses, whether sounding in tort, contract or otherwise, arising from or in connection with End User's, or End User's employees, contractors, or subcontractors, use of the DMF. This provision shall survive termination of the Agreement and will include any and all claims or liabilities arising from intellectual property rights

f. Liability:

    a. Neither credit reporting vendors nor the U.S. Government/NTIS (a) make any warranty, express or implied, with respect to information provided under this Section of the Policy, including, but not limited to, implied warranties of merchantability and fitness for any particular use; (b) assume any liability for any direct, indirect or consequential damages flowing from any use of any part of the DMF, including infringement of third party intellectual property rights; and (c) assume any liability for any errors or omissions in the DMF. The DMF does have inaccuracies and NTIS and the Social Security Administration (SSA), which provides the DMF to NTIS, does not guarantee the accuracy of the DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on the DMF is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the DMF.

    b. If an individual claims that SSA has incorrectly listed someone as deceased (or has incorrect dates/data on the DMF), the individual should be told to contact to their local Social Security office (with proof) to have the error corrected. The local Social Security office will:

        i. Make the correction to the main NUMIDENT file at i. SSA and give the individual a verification document of SSA's current records to use to show any company, recipient/purchaser of the DMF that has the error; OR,

        ii. Find that SSA already has the correct information ii. on the main NUMIDENT file and DMF (probably corrected sometime prior), and give the individual a verification document of SSA's records to use to show to any company subscriber/ purchaser of the DMF that had the error.

Birchwood
CREDIT SERVICES, INC.

Addendum C-1

Trans Union Requirements

Customer, in order to receive consumer credit information from Trans Union, LLC, through CRA, agrees to comply with the following conditions required by Trans Union, which may be in addition to those outlined in the Customer Service Agreement ("Agreement"). Customer understands and agrees that Trans Union's delivery of information to Customer via CRA is specifically conditioned upon Customer's agreement with the provisions set forth in this Agreement. Customer understands and agrees that these requirements pertain to all of its employees, managers and owners and that all persons having access to Trans Union consumer credit information, whether existing or future employees, will be trained to understand and comply with these obligations.

1. Customer certifies that Customer shall use the consumer reports: (a) solely for the Subscriber's certified use(s); and (b) solely for Customer's exclusive one-time use. Customer shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with Customer's own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by, and disclosed by Customer only to Customer's designated and authorized employees having a need to know and only to the extent necessary to enable Customer to use the Consumer Reports in accordance with this Agreement. Customer shall ensure that such designated and authorized employees shall not attempt to obtain any Consumer Reports on themselves, associates, or any other person except in the exercise of their official duties.

2. Customer will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.

3. Customer shall use each Consumer Report only for a one-time use and shall hold the report in strict confidence, and not disclose it to any third parties; provided, however, that Customer may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, unless otherwise explicitly authorized in an agreement between Reseller and its Customer for scores obtained from TransUnion, or as explicitly otherwise authorized in advance and in writing by TransUnion through Reseller, Customer shall not disclose to consumers or any third party, any or all such scores provided under such agreement, unless clearly required by law.

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

5. Customer will request Scores only for Customer's exclusive use. Customer may store Scores solely for Customer's own use in furtherance of Customer's original purpose for obtaining the Scores. Customer shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person except (i) to those employees of Customer with a need to know and in the course of their employment; (ii) to those third party processing agents of Customer who have executed an agreement that limits the use of the Scores by the third party to the use permitted to Customer and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; or (iv) to government regulatory agencies; or (v) as required by law.

6. Customer hereby agrees to comply with all current and future policies and procedures instituted by CRA and required by Trans Union. CRA will give Customer as much notice as possible prior to the effective date of any such new policies required in the future, but does not guarantee that reasonable notice will be possible. Customer may terminate this agreement at any time after notification of a change in policy in the event Customer deems such compliance as not within its best interest.

7. Customer certifies that it is not a reseller of the information, a private detective, bail bondsman, attorney, credit counseling firm, financial counseling firm, credit repair clinic, pawn shop (except companies that do only Title pawn), check cashing company, genealogical or heir research firm, dating service, massage or tattoo service, business that operates out of an apartment, an individual seeking information for his private use, an adult entertainment service of any kind, a company that locates missing children, a company that handles third party repossession, a company seeking information in connection with time shares or subscriptions, a company or individual involved in spiritual counseling or a person or entity that is not an end-user or decision-maker, unless approved in writing by Trans Union.

8. Customer agrees that Trans Union shall have the right to audit records of Customer that are relevant to the provision of services set forth in this agreement. Customer authorizes CRA to provide to Trans Union, upon Trans Union's request, all materials and information relating to its investigations of Customer and agrees that it will respond within the requested time frame indicated for information requested by Trans Union regarding Trans Union information. Customer understands that Trans Union may require CRA to suspend or terminate access to Trans Union's information in the event Customer does not cooperate with any such an investigation. Customer shall remain responsible for the payment for any services provided to Customer prior to any such discontinuance.

9. Customer agrees that Trans Union information will not be forwarded or shared with any third party unless required by law or approved by Trans Union. If approved by Trans Union and authorized by the consumer, Customer may deliver the consumer credit information to a third party, secondary, or joint user with which Customer has an ongoing business relationship for the permissible use of such information. Customer understands that Trans Union may charge a fee for the subsequent delivery to secondary users.

10. Trans Union shall use reasonable commercial efforts to obtain, assemble and maintain credit information on individuals as furnished by its subscribers or obtained from other available sources. THE WARRANTY SET FORTH IN THE PREVIOUS SENTENCE IS THE SOLE WARRANTY MADE BY TRANS UNION CONCERNING THE CONSUMER REPORTS, INCLUDING, BUT NOT LIMITED TO THE TU SCORES. TRANS UNION MAKES NO OTHER REPRESENTATIONS OR WARRANTIES INCLUDING, BUT NOT LIMITED TO, ANY REPRESENTATIONS OR WARRANTIES REGARDING THE ACCURACY, COMPLETENESS, OR BOTH, OF ANY AND ALL OF THE AFOREMENTIONED PRODUCTS AND SERVICES THAT MAY BE PROVIDED TO CRA. THE WARRANTY SET FORTH IN THE FIRST SENTENCE OF THIS PARAGRAPH IS IN LIEU OF ALL OTHER WARRANTIES, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, BUT NOT LIMITED TO, WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Birchwood
CREDIT SERVICES, INC.

Addendum C-2

TRANS UNION[SM] REQUIREMENTS REGARDING CREDIT SCORING SERVICES

CLASSIC CREDIT RISK SCORE SERVICES

(Required Terms for Addendum to Subscriber Agreement for Consumer Reports between Reseller and its Customer)

1. Based on an agreement with Trans Union LLC ("Trans Union") and Fair Isaac Corporation ("Fair Isaac") ("Reseller Agreement"), CRA has access to a unique and proprietary statistical credit scoring service jointly offered by Trans Union and Fair Isaac which evaluates certain information in the credit reports of individual consumers from Trans Union's data base ("Classic") and provides a score which rank orders consumers with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring (the "Classic Score").

2. Customer, from time to time, may desire to obtain Classic Scores from Trans Union via an on-line mode in connection with consumer credit reports.

3. Customer has previously represented and now, again represents that it is a _____ _____and has a permissible purpose for obtaining consumer reports, as defined by Section 604 of the Federal Fair Credit Reporting Act (15 USC 1681b) including, without limitation, all amendments thereto ("FCRA").

4. Customer certifies that it will request Classic Scores pursuant to procedures prescribed by CRA from time to time only for the permissible purpose certified above, and will use the Classic Scores obtained for no other purpose.

5. Customer will maintain copies of all written authorizations for a minimum of three (3) years from the date of inquiry.

6. Customer agrees that it shall use each Classic Score only for a one-time use and only in accordance with its permissible purpose under the FCRA.

7. With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, CRA may, upon its election, discontinue serving the Customer and cancel this Agreement, in whole or in part (e.g., the services provided under this Addendum only) immediately.

8. Customer recognizes that factors other than the Classic Score may be considered in making a credit decision. Such other factors include, but are not limited to, the credit report, the individual account history, and economic factors.

9. Trans Union and Fair Isaac shall be deemed third party beneficiaries under this Addendum.

10. Up to five score reason codes, or if applicable, exclusion reasons, are provided to Customer with Classic Scores. These score reason codes are designed to indicate the reasons why the individual did not have a higher Classic Score, and may be disclosed to consumers as the reasons for taking adverse action, as required by the Equal Credit Opportunity Act ("ECOA") and its implementing Regulation ("Reg. B"). However, the Classic Score itself is proprietary to Fair Isaac, may not be used as the reason for adverse action under Reg. B and, accordingly, shall not be disclosed to credit applicants or any other third party, except: (1) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (2) as clearly required by law. Customer will not publicly disseminate any results of the validations or other reports derived from the Classic Scores without Fair Isaac and Trans Union's prior written consent.

11. In the event Customer intends to provide Classic Scores to any agent, Customer may do so provided, however, that Customer first enters into a written agreement with such agent that is consistent with Customer's obligations under this Agreement. Moreover, such agreement between Customer and such agent shall contain the following obligations and acknowledgments of the agent: (1) Such agent shall utilize the

Classic Scores for the sole benefit of Customer and shall not utilize the Classic Scores for any other purpose including for such agent's own purposes or benefit; (2) That the Classic Score is proprietary to Fair Isaac and, accordingly, shall not be disclosed to the credit applicant or any third party without Trans Union and Fair Isaac's prior written consent except (a) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (b) as clearly required by law; (3) Such Agent shall not use the Classic Scores for model development, model validation, model benchmarking, reverse engineering, or model calibration; (4) Such agent shall not resell the Classic Scores; and (5) Such agent shall not use the Classic Scores to create or maintain a database for itself or otherwise.

12. Customer acknowledges that the Classic Scores provided under this Agreement which utilize an individual's consumer credit information will result in an inquiry being added to the consumer's credit file.

13. Customer shall be responsible for compliance with all applicable federal or state legislation, regulations and judicial actions, as now or as may become effective including, but not limited to, the FCRA, the ECOA, and Reg. B, to which it is subject.

14. The information including, without limitation, the consumer credit data, used in providing Classic Scores under this Agreement were obtained from sources considered to be reliable. However, due to the possibilities of errors inherent in the procurement and compilation of data involving a large number of individuals, neither the accuracy nor completeness of such information is guaranteed. Moreover, in no event shall Trans Union, Fair Isaac, nor their officers, employees, affiliated companies or bureaus, independent contractors or agents be liable to Customer for any claim, injury or damage suffered directly or indirectly by Customer as a result of the inaccuracy or incompleteness of such information used in providing Classic Scores under this Agreement and/or as a result of Customer's use of Classic Scores and/or any other information or serviced provided under this Agreement.

15.1 Fair Isaac, the developer of Classic, warrants that the scoring algorithms as delivered to Trans Union and used in the computation of the Classic Score ("Models") are empirically derived from Trans Union's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring when applied to the population for which they were developed, and that no scoring algorithm used by Classic uses a "prohibited basis" as that term is defined in the Equal Credit Opportunity Act (ECOA) and Regulation B promulgated there under. Classic provides a statistical evaluation of certain information in Trans Union's files on a particular individual, and the Classic Score indicates the relative likelihood that the consumer will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring relative to other individuals in Trans Union's database. The score may appear on a credit report for convenience only, but is not a part of the credit report nor does it add to the information in the report on which it is based.

15.2 THE WARRANTIES SET FORTH IN SECTION 15.1 ARE THE SOLE WARRANTIES MADE UNDER THIS ADDENDUM CONCERNING THE CLASSIC SCORES AND ANY OTHER DOCUMENTATION OR OTHER DELIVERABLES AND SERVICES PROVIDED UNDER THIS AGREEMENT; AND NEITHER FAIR ISAAC NOR TRANS UNION MAKE ANY OTHER REPRESENTATIONS OR WARRANTIES CONCERNING THE PRODUCTS AND SERVICES TO BE PROVIDED UNDER THIS AGREEMENT OTHER THAN AS SET FORTH IN THIS ADDENDUM. THE WARRANTIES AND REMEDIES SET FORTH IN SECTION 15.1 ARE IN LIEU OF ALL OTHERS, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT MIGHT BE IMPLIED FROM ACOURSE OF PERFORMANCE OR DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

16. IN NO EVENT SHALL ANY PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES INCURRED BY THE OTHER PARTIES AND ARISING OUT OF THE PERFORMANCE OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LOSS OF GOOD WILL AND LOST PROFITS OR REVENUE, WHETHER OR NOT SUCH LOSS OR DAMAGE IS BASED IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY, OR OTHERWISE, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

17. THE FOREGOING NOTWITHSTANDING, WITH RESPECT TO CUSTOMER, IN NO EVENT SHALL THE AFORESTATED LIMITATIONS OF LIABILITY, SET FORTH ABOVE IN SECTION 16, APPLY TO

DAMAGES INCURRED BY TRANS UNION AND/OR FAIR ISAAC AS A RESULT OF: (A) GOVERNMENTAL, REGULATORY OR JUDICIAL ACTION(S) PERTAINING TO VIOLATIONS OF THE FCRA AND/OR OTHER LAWS, REGULATIONS AND/OR JUDICIAL ACTIONS TO THE EXTENT SUCH DAMAGES RESULT FROM CUSTOMER'S BREACH, DIRECTLY OR THROUGH CUSTOMER'S AGENT(S), OF ITS OBLIGATIONS UNDER THIS AGREEMENT.

18. ADDITIONALLY, NEITHER TRANS UNION NOR FAIR ISAAC SHALL BE LIABLE FOR ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS ADDENDUM BROUGHT MORE THAN ONE (1) YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED. IN NO EVENT SHALL TRANS UNION'S AND FAIR ISAAC'S AGGREGATE TOTAL LIABILITY, IF ANY, UNDER THIS AGREEMENT, EXCEED THE AGGREGATE AMOUNT PAID, UNDER THIS ADDENDUM, BY CUSTOMER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING ANY SUCH CLAIM, OR TEN THOUSAND DOLLARS ($10,000.00), WHICHEVER AMOUNT IS LESS.

19. This Addendum may be terminated automatically and without notice: (1) in the event of a breach of the provisions of this Addendum by Customer; (2) in the event the agreement(s) related to Classic between Trans Union, Fair Isaac and CRA are terminated or expire; (3) in the event the requirements of any law, regulation or judicial action are not met, (4) as a result of changes in laws, regulations or regulatory or judicial action, that the requirements of any law, regulation or judicial action will not be met; and/or (5) the use of the Classic Service is the subject of litigation or threatened litigation.