Fair Information Practices ("FIP").

Restrictions on State Department of Motor Vehicle or its Outsourced Providers Data ("DMV Data")

Please Note: The following terms and conditions apply to any DMV Data ordered and/or received from LexisNexis Risk Solutions Inc. on behalf of itself and its affiliates ("LexisNexis"). You (on behalf of yourself and your insurance organization and your affiliates) ("Customer") agree that ordering and/or use of any such DMV Data represents (a) your acknowledgement of these terms, (b) that you are authorized to act on behalf of and bind your organization, and (c) your affirmative agreement to be bound by the following:

1. **GENERAL TERMS.**
   1.1. Customer shall not use any LexisNexis provided MVR, or portions of information contained therein, to create, link, or update a file such that Customer develops its own source of driving history information.
   1.2. **State Forms.** As requested by LexisNexis, Customer shall complete any state forms that LexisNexis is legally or contractually bound to obtain from Customer before serving Customer with DMV Data.
   1.3. **Customer Data Retention Requirements.** In Colorado, Idaho (Monitoring), Maryland, New Mexico, Pennsylvania and West Virginia Customer must keep and maintain, in accordance with commercially reasonable confidential data archive standards and state and federal law, for a period of time equal to five (5) years after the date any DMV Data is acquired in the foregoing states from LexisNexis books and records of all transactions conducted under your agreement with LexisNexis for services, including financial accounts:
      a) Documenting disclosure of any DMV Data in or under its possession or control;
      b) Documenting its systems and operation for handling of and safeguarding from unauthorized disclosure of DMV Data under your agreement with LexisNexis for services;
      c) Documenting its compliance with the other terms and conditions of your agreement with LexisNexis for services;
      d) Documenting each authorized recipient’s permitted use and purpose for obtaining each record, if applicable; and
      e) Customer will make available to LexisNexis or the DMV (or such parties’ authorized representatives) all such books and records including financial accounts, for auditing, compliance and monitoring purposes. LexisNexis or the DMV (or such parties’ authorized representative) shall have the right, but not the obligation, to conduct any inquiry or audit hereunder at any time.

2. **INTERNET ADDENDUM.** Customer must execute an Internet Addendum with LexisNexis before distributing Pennsylvania, Washington and West Virginia MVRs to its agents via the Internet. For all other states, if Customer provides DMV Data access to its agents or employees via an Internet website, Customer shall ensure that such website uses current security technologies such as encryption, firewall, logo, and password technology to protect access to such DMV Data from any and all users except authorized users.
Fair Information Practices (“FIP”).

3. **WRITTEN CONSENT REQUIRED.**
   3.1. Without limiting the foregoing, Customer shall comply with the Vermont Fair Credit Reporting Act, 9 V.S.A. § 2480e, by securing the consent of the subject consumer prior to ordering a consumer report on a Vermont resident.
   3.2. If Customer orders an MVR from Alaska or Puerto Rico for any purpose, Customer shall obtain the written authorization of the subject consumer before ordering such MVR.
   3.3. If Customer orders an MVR from Arizona for life and or health insurance purposes, Customer shall obtain the written authorization of the consumer before ordering such MVR.
   3.4. With regard to MVRs originating from Arkansas, written authorization must be obtained if the MVR does not involve the insurer’s own insured or applicant or a licensed driver in the household of the insured or applicant.
   3.5. In Georgia, Customer cannot order MVRs on third-party claimants that are not also their insured unless written authorization is first obtained.

4. **INDEMNIFICATION.** With regard to MVRs from Colorado, Idaho, Indiana, New Mexico, Pennsylvania and West Virginia:
   Customer agrees to indemnify, hold harmless, and release State of Colorado, Idaho.gov and the State of Idaho, Indiana.gov and the State of Indiana, New Mexico Interactive and the State of New Mexico, the State of Pennsylvania, Pennsylvania Interactive and their respective parent corporations, subsidiaries, officers, agents, agencies, contractors, and subcontractors and employees (collectively, the “Releaseses”) from and against any and all loss, damages of any kind, injury, liability, court awards, suits and proceedings, including costs, expenses and attorneys’ fees, arising from the provision or receipt of the respective State’s DMV Data, except insofar (with respect to the State of Colorado, the State of Idaho, the State of Indiana, the State of New Mexico, and the State of West Virginia) as they may result from the actions or inactions of the State or its outsource provider and each of their parent corporation, their subsidiaries, officers, agents, contractors, subcontractors, or employees.

5. **SYSTEM AND DATA SECURITY PROCEDURES.**
   For the states of Colorado, Idaho (Monitoring) and Maryland, Customer must implement reasonable system and data security procedures to protect DMV Data from unauthorized disclosure. Such reasonable procedures must include, but are not limited to, username and password access policies, firewalls, background investigations of employees or any other individuals authorized to access driver’s license records, appropriate protection of data during transmission using techniques such as VPNs, private point-to-point connections, or encryption, and execution of confidentiality agreements by employees or other individuals with authorized access.

6. **REMEDIAL ACTION.**
   For the states of Colorado, Idaho (Monitoring), Maryland, New Mexico and Pennsylvania, Customer is subject to remedial action by the state or third-party vendor or both, in the event of violation of the terms and conditions contained in this FIP and/or your agreement with LexisNexis for services. Such remedial action may range from suspension for a fixed period of time from receiving DMV Data, to termination of the privilege of receiving DMV Data, and may include liability of Customer for actual damages, attorneys’ fees and costs, and interest as
Fair Information Practices ("FIP").

permitted by law.

In addition to the terms and conditions set forth above, the following are state-specific requirements:

7. **ALASKA.** See Written Consent Required in Section 3.

8. **ARIZONA.** See Written Consent Required in Section 3.

9. **ARKANSAS.** An insurer may obtain a commercial record if it is on a commercial policy and the licensee is a commercial driver (Class A, B or C). If the licensee is a Class D driver, the insurance company can pull an insurance record, but can only pull a commercial record if signed authorization is obtained. See additional restriction under Written Consent Required in Section 3.

10. **COLORADO.** See Consumer Data Retention Requirements in Section 1, Indemnification in Section 4, System and Data Security Procedures in Section 5, and Remedial Action in Section 6 for restrictions.

11. **GEORGIA.** Customer may not order Georgia MVRs for health insurance purposes. See also Written Consent in Section 3 for additional restriction.

12. **HAWAII.** When ordering an MVR on an individual under the age of 18, Customer must order the MVRs manually from the State. Customer must mail an original Juvenile Information Release Form, and a check to: Traffic Violations Bureau, Attn: Abstract Department, 1111 Alakea Street, Honolulu, HI 96813.

13. **IDAHO MONITORING.** Customer may only use the Idaho DMV Data for activities directly related to the re-underwriting of motor vehicle insurance policies. See also Consumer Data Retention Requirements in Section 1, Indemnification in Section 4, System and Data Security Procedures in Section 5, and Remedial Action in section 6 for additional restrictions.

14. **INDIANA.** See Indemnification in Section 4 for restriction.

15. **MARYLAND.** See Consumer Data Retention Requirements in Section 1, System and Data Security Procedures in Section 5 and Remedial Action in Section 6 for restrictions.

16. **NEW HAMPSHIRE.**
   16.1. DMV Data derived from the New Hampshire Department of Safety is governed by N.H. Statute § 260:14. Section 260:14(IX) provides for penalties to be assessed against an individual in the event such individual improperly discloses, uses, obtains, sells, rents, offers or exposes for sale New Hampshire DMV Data.
   16.2. Customer may not order New Hampshire MVRs for health insurance purposes.
   16.3. Insurance companies must be authorized to write automobile and personal excess liability insurance in New Hampshire to obtain MVRs for automobile insurance or
personal liability insurance unless the Customer is an affiliate or subsidiary of another insurance company that is authorized to write automobile insurance or personal liability insurance in New Hampshire.

16.4. Insurance companies authorized in New Hampshire to write life insurance policies in the state, or their authorized agents, may obtain MVRs for use in connection with the underwriting or rating of a life insurance policy, as long as the insurer provides the individual with written notice.

17. NEW MEXICO. See Customer Data Retention Requirements in Section 1, Indemnification in Section 4, and Remedial Action in Section 6 for restrictions.

18. PENNSYLVANIA. See Customer Data Retention Requirements in Section 1, Internet Addendum in Section 2, Indemnification in Section 4, and Remedial Action in Section 6 for restrictions.

19. PUERTO RICO. See Written Consent Required in Section 3.

20. UTAH. Customers who request MVRs and/or the Monitoring Service must sign the Terms and Conditions found at http://secure.utah.gov.dhr. MVRs and the Monitoring Service can only be used for Auto insurance purposes. Utah MVRs and the Monitoring Service cannot be used for Life, Health or Home purposes.

21. VERMONT. See Written Consent Required in Section 3.

22. WASHINGTON. Washington MVRs or any parts thereof shall be used for motor vehicle insurance underwriting only and no information contained therein is to be used for any other purpose or divulged, sold, assigned or otherwise transferred to any third party including a reinsurer.

   22.1. An insurance carrier or agent shall order a non-commercial Washington MVR only when it has motor vehicle insurance in effect covering the named individual or when the named individual has applied to the insurance carrier or agent for such insurance or when the insurance carrier or agent has motor vehicle insurance in effect covering the employer or prospective employer where the person is employed to operate a "commercial vehicle" upon the public highways as defined in RCW 46.04.140, other than a "commercial motor vehicle" as defined in RCW 46.25.010(6).

   22.2. An insurance carrier or agent shall order a commercial Washington MVR only when it has motor vehicle insurance in effect covering the employer or a prospective employer where the person is employed to operate a "commercial motor vehicle" upon the public highways as defined in Chapter 46.25.016(6) RCW or to the insurance carrier or agent to which the employer or prospective employer has applied.

   22.3. An insurance carrier or agent shall order a life MVR only when it has life insurance in effect covering the named individual, or the named individual has applied to insurance carrier or its agent for such insurance. Washington life MVRs or any parts thereof shall not be divulged, sold, assigned or otherwise transferred to any third party including a reinsurer.

   22.4. Customer may not order Washington MVRs for health insurance purposes, nor may Washington MVRs be used for claims investigation purposes.
Fair Information Practices ("FIP").

22.5. See Internet Addendum in Section 2 for additional restriction.

23. **WEST VIRGINIA.** See Customer Data Retention Requirements in Section 1, Internet Addendum in Section 2, and Indemnification in Section 4 for additional restrictions.

**OTHER TERMS AND CONDITIONS.**

**Please Note:** The following terms and conditions only apply if your insurance organization’s contract ("Agreement") with LexisNexis Risk Solutions Inc. on behalf of itself and its affiliates ("LexisNexis") does not contain these specific clauses. Provided, however, if such clauses have been included and negotiated by LexisNexis and your organization in the Agreement, the clauses contained in the Agreement shall control over the terms contained herein. To the extent the clauses apply to you, you (on behalf of yourself and your organization and your affiliates) ("Customer") agree that ordering and/or use of any LexisNexis products and services represents (a) your acknowledgement of these terms, (b) that you are authorized to act on behalf of and bind your organization, and (c) your affirmative agreement to be bound by the following:

1. **Terms and Conditions related to FCRA-Governed Services.**
   1.1. For all services obtained from LexisNexis, using its proprietary databases and information obtained from third parties under the Agreement that qualify as consumer reports under the FCRA, Customer shall comply with the requirements of the FCRA, including first obtaining written authorization of the consumer where required. In addition to the foregoing, with respect to consumers resident in the State of Vermont, Customer must comply with the Vermont Fair Credit Reporting Act, 9 V.S.A. §2480e.
   
   1.2. Customer acknowledges it has reviewed and shall comply with the “Notice To Users Of Consumer Reports”, attached hereto as Appendix 1, and may also be accessed www.consumerfinance.gov/learnmore which informs users of consumer reports of their legal obligations under the FCRA.

2. **DPPA.** Driver’s Privacy Protection Act. Customer acknowledges that certain services provided by LexisNexis may include the provision of certain personal information data from a motor vehicle record obtained by LexisNexis from state Departments of Motor Vehicles and its outsourced providers (“DMV Data”) and that such DMV Data is governed by as those terms are defined by the Federal Driver’s Privacy Protection Act, 18 U.S.C. § 2721 et seq., (“DPPA”) and its state analogues ("DMV Data"), and that Customer is required to comply with the DPPA or state analogues, as applicable. Customer agrees that it may be required to certify its permissible use of DPPA or DMV Data at the time it requests information in connection with certain services and will recertify upon request by LexisNexis.

3. **AUDIT AND CREDENTIALING.**
   3.1. LexisNexis Audit Rights. LexisNexis may conduct periodic reviews of Customer related to Customer’s use of services provided by LexisNexis. In addition, LexisNexis may, upon reasonable notice, audit Customer’s records, premises, processes and procedures related to its use, storage and disposal of the services and information received from LexisNexis. Further, certain third party data providers, such as Departments of Motor
Fair Information Practices (“FIP”).

Vehicles or its outsourced providers (“DMV”) and credit bureaus, require the right to audit Customer, either directly or through LexisNexis, and Customer consents to such third party audits as a condition to receive data derived from such third parties. Customer agrees to cooperate fully with any and all reviews and provide responses within any designated timeframes. Any violations discovered as a result of such audit or failure to respond to an audit request may cause for immediate action by LexisNexis, including, but not limited to, immediate termination of any applicable agreement with LexisNexis, termination of the right to use any LexisNexis services, reactivation fees, legal action, and/or referral to federal or state regulatory agencies.

3.2. LexisNexis Credentialing Rights. Customer agrees to credentialing (or re-credentialing), by LexisNexis, to ensure Customer is a legitimate business entity with permissible purpose to order and receive the services from LexisNexis. If Customer fails to meet or continue to meet LexisNexis credentialing requirements, in LexisNexis’s sole discretion, LexisNexis may take immediate action, including, but not limited to, immediate termination of any applicable agreement with LexisNexis, termination of the right to use any services, reactivation fees, legal action, and/or referral to federal or state regulatory agencies.

4. CUSTOMER DATA RETENTION REQUIREMENTS.

4.1. For all services provided under this FIP or your applicable agreement with LexisNexis, Customer shall maintain complete and accurate records, including (i) the identity of the individual or entity ordering the report (ii) the consumer’s name, and (iii) the purpose for order, for a period of five (5) years unless longer retention is required by LexisNexis third party data provider requirements or state or federal law. In addition, if a report is ordered to provide an insurance quote, Customer must also maintain a record of the type of policy involved. Within seven (7) days of a LexisNexis or DMV request, Customer shall generate a report with the history of its disclosures of any DMV Data provided by LexisNexis.
Appendix 1

Notice To Users Of Consumer Reports

All users of consumer reports must comply with all applicable regulations. 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 Consumer Financial Protection Bureau’s ("CFPB") 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 CFPB’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)
Fair Information Practices ("FIP").

- 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 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 identity 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 consumer’s file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are 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. Federal regulations have been issued that cover disposal.

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 CFPB. 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.
Fair Information Practices ("FIP").

- 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 federal regulations) – 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 615(d). This practice is known as “prescreening” and typically involves obtaining from a CRA a list of consumers who meet certain pre-established 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 CFPB has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The 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 CFPB’s website, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA. Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1618 et seq.:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>602</td>
<td>1681</td>
<td>603</td>
<td>1681a</td>
<td>604</td>
<td>1681b</td>
</tr>
<tr>
<td>605</td>
<td>1681c</td>
<td>605A</td>
<td>1681cA</td>
<td>605B</td>
<td>1681cB</td>
</tr>
<tr>
<td>606</td>
<td>1681d</td>
<td>607</td>
<td>1681e</td>
<td>608</td>
<td>1681f</td>
</tr>
<tr>
<td>609</td>
<td>1681g</td>
<td>610</td>
<td>1681h</td>
<td>611</td>
<td>1681i</td>
</tr>
<tr>
<td>612</td>
<td>1681j</td>
<td>613</td>
<td>1681k</td>
<td>614</td>
<td>1681l</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Section 615 1681n
Section 616 1681o
Section 617 1681p
Section 618 1681q
Section 619 1681r
Section 620 1681s
Section 621 1681s-1
Section 622 1681s-2
Section 623 1681u
Section 624 1681v
Section 625 1681w
Section 626 1681x
Section 627 1681y