

ADDENDUM TO ORDER FORM FOR SPECIAL SERVICES

This Addendum ("Addendum") is incorporated into and made part of the Order Form entered into between Inovalon Provider, Inc. ("INOVALON") and Customer, and whose head office is located at the address set forth in the Order Form, pursuant to which INOVALON makes available certain services to Customer (hereinafter referred to as "End User").

End User desires to obtain certain fraud prevention services, including ID Verification and Demographic Verification (the "ID Services") and certain services that are derivative of, and are treated as, consumer credit reports (the "Credit Services"), which are offered by INOVALON pursuant to its arrangements with a national consumer reporting agency, all pursuant to the terms and conditions set forth in this Addendum. The ID Services and the Credit Services are collectively referred to herein as the "Special Services".

Accordingly, the parties hereby agree as follows:

1. This Addendum is incorporated into and made a part of the Order Form by and between INOVALON and Customer. The Order Form, as modified by this Addendum, including any annexes hereto and documents referenced herein, the Service Agreement or Master Agreement and any Business Associate Agreement ("BAA") entered into by the parties, shall comprise the entire agreement of the parties hereto (as used herein, "Agreement"). Except as expressly set forth herein, the Agreement shall remain unmodified and in full force and effect. In the event of any conflict among the Agreement and this Addendum with respect to the Special Services, the terms of this Addendum shall control.

2. End User understands that the Special Services are provided pursuant to and in accordance with the requirements of a consumer reporting agency (the "CRA"). INOVALON may from time to time enter into arrangements with other consumer reporting agencies that provide services that are functionally the equivalent of the Special Services and may provide such services to End User in replacement of the Special Services pursuant to this Addendum, which shall continue in full force and effect. The End User will cooperate with INOVALON to implement procedural changes, if any, that may be required to access the Special Services. User further understands and agrees that INOVALON will disclose the End User's identity and such other information concerning the use of the Special Services as the CRA may require as a condition of obtaining the services and/or to comply with law. End User agrees to comply with all terms and guidelines contained in CRA user guides and other related documentation (together, the "CRA Documentation") provided by the CRA directly or through INOVALON in connection with the Special Services. End User further agrees that it will not make any use whatsoever of CRA's name or logo or other registered trade or service marks.

3. With respect to each End User request for Special Services, End User and its employees and agents shall comply with all applicable federal, state and local laws, statutes, rules and regulations including, but not limited to: (a) the Fair Credit Reporting Act ("FCRA"), 12 U.S.C. §1681 et seq., and Regulation V of the Consumer Financial Protection Bureau ("CFPB"), 12 C.F.R. Part 1022 ("Regulation V") promulgated thereunder, (b) Title V of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801 et seq., the CFPB's Regulation P ("Regulation P"), 12 C.F.R. Part 1016, and the Federal Trade Commission's ("FTC's") Privacy of Consumer Financial Information rule (the "FTC Rule"), 16 C.F.R. Part 313, each promulgated thereunder, and (c) all other applicable privacy laws, and similar State laws and regulations, as all of the above may be amended and interpreted from time to time by competent legislative, regulatory or judicial authority. End User acknowledges and agrees that information obtained by End User through the Special Services includes "nonpublic personal information" ("NPPI") of "consumers" as defined for purposes of the FCRA, the GLB Act and the regulations promulgated thereunder.

4. Provisions applicable to the Credit Services:

4.1. End User is a lawfully registered legal entity and has a permissible purpose for obtaining consumer reports in accordance with the FCRA. The End User covenants with and certifies to INOVALON that its permissible purpose in obtaining the Credit Services is in accordance with one or more of the following:

- a) In connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of the consumer; or
- b) In accordance with the written instructions of the consumer; or

- c) For a legitimate business need in connection with a business transaction that is initiated by the consumer; and/or
- d) As a potential investor, servicer or current insurer in connection with a valuation of, or assessment of, the credit or prepayment risks.

4.2. End User covenants with and certifies to INOVALON that it shall use the consumer reports: (a) solely for the End User's certified use(s); and (b) solely for End User's exclusive one-time use. End User 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 Addendum to any other party, whether alone, in conjunction with End User's own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by and only disclosed by End User to its designated and authorized employees having a need to know and only to the extent necessary to enable End User to use the consumer reports in accordance with this Addendum. End User 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.

4.3. THE FCRA PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18 OF THE UNITED STATES CODE OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.

4.4. End User 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 End User 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, End User shall not disclose to consumers or any third party, any or all Scores (as defined herein) provided under this Addendum, unless clearly required by law.

4.5. The Credit Services include a "propensity to pay" score which is based in part on credit related scores derived from consumer credit reports (collectively, "Scores"). End User agrees that it will request Scores only for End User's exclusive use. End User may store Scores solely for End User's own use in furtherance of End User's original purpose for obtaining the Scores. End User shall not use the Scores for model development or model calibration and shall not reverse engineer the Scores. 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 or entity except (i) to those employees of End User with a need to know and in the course of their employment; (ii) to those third party processing agents and other contractors of End User who have executed an agreement that limits the use of the Scores by the third party only to the use permitted to End User and contains the prohibitions set forth herein regarding model development, model calibration, reverse engineering and confidentiality; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; (iv) to government regulatory agencies; or (v) as required by law.

4.6. End User acknowledges receipt of a copy of the CFPB's "Notice to Users of Consumer Reports -- Obligations of Users Under the FCRA" attached hereto as **Annex 3**.

5. Provisions applicable to the ID Services:

5.1. End User covenants with and certifies to INOVALON that End User is, and will be, the sole user of the ID Services and that End User and its employees may request, obtain and use such services only to protect against or prevent actual fraud, unauthorized transactions, claims or other liability (the "GLB Permitted Use"). It is understood that End User will use the ID Services for the GLB Permitted Use in the normal course of its business to verify the accuracy of information submitted by consumers and to correct any misinformation provided, all in furtherance of the GLB Permitted Use. End User will not request, obtain, or use ID Services for marketing purposes nor for any other purpose, except the GLB Permitted Use. End User further acknowledges and agrees that the ID Services are not "consumer reports" within the meaning of the FCRA. End User agrees and hereby covenants with and certifies to INOVALON (i) that it shall not use ID Services, in whole or in part, as a factor in establishing a consumer's creditworthiness or eligibility for credit, insurance, employment, or for any other permitted purpose under the FCRA and (ii) it shall not take any adverse action based in whole or in part on the ID Services against any consumer. For the purposes of this Addendum, the terms "adverse action" and "consumer" shall have the meanings ascribed to such terms by the FCRA.

5.2. End User covenants with and certifies to INOVALON that End User shall use the ID Services solely for End User's exclusive one-time use for the GLB Permitted Use and shall hold the information obtained through such services in strict confidence. End User shall not request, obtain or distribute ID Services for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Addendum to any other party, whether alone, in conjunction with End User's own data, or otherwise in any service which is derived from the ID Services. The ID Services shall be requested by and only disclosed by End User to End User's designated and authorized employees having a need to know and only to the extent necessary to enable End User to use the Reference Services in accordance with this Agreement. End User shall ensure that such designated and authorized employees shall not attempt to obtain any ID Services on themselves, associates, or any other person except in the exercise of their official duties.

6. Provisions applicable to all Special Services

6.1. End User agrees to furnish all information required by INOVALON and CRA to verify its identity, as set forth in Annex 1 hereto, and to provide additional information from time to time as may be requested by INOVALON. End User agrees that INOVALON or its designee may perform an on-site inspection of End User to ensure that the proposed use of the Special Services is consistent with End User's stated purposes for obtaining such services. End User shall maintain commercially reasonable records including, but not limited to complete and accurate accounting records in accordance with generally accepted accounting practices, to substantiate End User's performance under this Addendum with respect to the Special Services, including, without limitation, End User's compliance with payment, legal and all security requirements. End User shall preserve such records both during and for a period of at least five (5) years after termination of this Addendum and shall provide copies of such records and information to INOVALON as may be reasonably requested from time to time. Additionally, End User agrees that INOVALON or its designee may audit End User to ensure its compliance with the provisions of this Addendum. The cost of any such audit shall be borne by End User.

6.2. End User shall obtain a consumer authorization with respect to the Special Services that contains, at a minimum, the individual's name, address, social security number (where available) and legally enforceable electronic or written authorization or signature. End User shall maintain copies of all such written authorizations for a minimum of five (5) years from the date of inquiry and make such authorizations available to INOVALON and its vendor upon written request. Failure to furnish evidence of an authorization to INOVALON and its vendor upon request will be deemed a material breach of this Addendum and grounds for termination of the Agreement.

6.3. This Addendum shall become effective on the date agreed to by the parties as set forth within the relevant Order Form. This Addendum shall terminate upon termination of the Agreement. In addition to any grounds for termination set forth in the Agreement, INOVALON may terminate this Addendum and the provision of Special Services to End User, whether or not the Agreement is simultaneously terminated, if INOVALON or the CRA determine that the End User has breached the terms and conditions set forth herein, or should any of the certifications provided herein to INOVALON prove to have been false when made or have ceased to be true at any time that this Addendum is in effect. INOVALON may also immediately terminate this Addendum: (i) if for any reason the CRA ceases to provide the Special Services either generally or to INOVALON alone; and (ii) in the event any statute, regulation or other legal requirement governing the provision of the Special Services is changed in any manner that materially and adversely affects INOVALON's provision of the Special Services.

6.4. Because information provided hereunder includes NPPI, pursuant to the FTC Rule, End User must maintain a comprehensive information security program that is written in one or more readily accessible parts and contain administrative, technical, and physical safeguards that are appropriate to its size and complexity, the nature and scope of its activities, and the sensitivity of the NPPI. Such safeguards must be reasonably designed to (i) insure the security and confidentiality of NPPI, (ii) protect against any anticipated threats or hazards to the security or integrity of such information and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience. Among other things, the FTC Rule requires that the information security program (i) be coordinated by a designated employee or employees, (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of NPPI that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks in each relevant area of your operations. The information security program must be designed to and implement information safeguards to control the risks identified through the risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures. In addition, End User must oversee its service providers, by: (i) taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for NPPI to which it has access; and (ii) requiring such service providers by

contract to implement and maintain such safeguards. In addition, End User must periodically evaluate and adjust its information security program in light of (i) the results of testing and monitoring, (ii) any material changes to its operations or business arrangements, or (iii) any other circumstances that of which End User knows or has reason to know may have a material impact on its information security program.

6.5. End User covenants with and certifies to INOVALON that its information security program satisfies the foregoing requirements. End User further covenants with and certifies to INOVALON that its information security program complies with ISO27002:2005 international standards, as modified from time-to-time, in connection with the operation of its business and its performance under this Addendum. End User agrees to provide to INOVALON on request, from time to time, copies of End User's technical, administrative, and physical security and control policies and procedures that relate to NPPI furnished pursuant to this Addendum. From time to time INOVALON may request and End User shall also provide, at CRA's request, copies of End User's policies and procedures with respect to operations, incident response, problem management and change management, to the extent the foregoing pertain to this Addendum, and copies of any SSAE 16 Type II report regarding security controls and operations; provided however, that End User shall be under no obligation to obtain such SSAE 16 Type II report. In addition to the foregoing, End User must also comply with the End User Authentication Requirements set forth in **Annex 2** hereto.

6.6. Without limiting any other obligations of End User found herein, End User shall implement, and shall take all measures to maintain, commercially reasonable and appropriate administrative, technical and physical security safeguards ("Safeguards") designed to (a) ensure the security and confidentiality of all NPPI obtained in connection with the Special Services; (b) protect against any and all reasonably anticipated threats or hazards to the security or integrity of such services; and (c) protect against unauthorized access or use of such services and the information derived therefrom that could result in substantial harm or inconvenience to any consumer. End User shall immediately (but in no event later than twenty-four (24) hours after the occurrence of any of the following) notify INOVALON by phone and in writing in the event: (i) of any changes to End User's business, or in the event any other circumstances arise, which End User knows, or has reason to know, will have a material adverse impact on such Safeguards; (ii) End User becomes aware that its Safeguards are otherwise insufficient to meet its obligations hereunder, or (iii) End User becomes aware of any unauthorized disclosures, or other misappropriation, of any information provided to End User hereunder, including, but not limited to theft, loss or interception of the Special Services, unauthorized use of INOVALON or CRA-supplied identification codes and passwords, unauthorized entry to the facilities where Special Services data may have been accessible, or unauthorized release of or access to such data by an employee or agent of End User, resulting from a breach of End User's Safeguards or otherwise. End User shall cooperate fully with INOVALON and CRA in mitigating any damages due to any misappropriation or unauthorized use or disclosure of any Special Services or other information provided by INOVALON or CRA to End User. Such cooperation shall include, but not necessarily be limited to, allowing INOVALON and/or CRA to participate in the investigation of the cause and extent of such misappropriation and/or unauthorized disclosure. Such cooperation shall not relieve End User of any liability it may have as a result of such a misappropriation and/or unauthorized disclosure. End User agrees, that to the extent any such unauthorized use, unauthorized disclosure, misappropriation, or other event is due to End User's negligence, intentional wrongful conduct or breach of this Addendum, End User shall be responsible for any required consumer, public and/or other notifications, and all costs associated therewith; provided however, that except to the extent required to comply with applicable law, End User shall make no public notification, including but not limited to press releases or consumer notifications, of the potential or actual occurrence of such misappropriation and/or unauthorized disclosure without INOVALON's prior written consent. Failure of End User to fully cooperate with INOVALON in mitigating any damages due to any misappropriation or unauthorized use or disclosure of information provided through Special Services to End User may result in immediate suspension and/or termination of this Addendum by INOVALON, at its sole discretion.

6.7. In addition to any indemnification obligation under the Agreement of which this Addendum is a part, End User shall indemnify and hold INOVALON harmless from any and all claims, losses and damages, liability, and costs, including attorney's fees, against, or incurred by, INOVALON to the extent such claims, damages, liability and costs result directly or indirectly from either or both of the following: (a) any use of the Special Services; or (b) End User's breach of its obligations under this Addendum including, but not limited to, any breach which results in the non-permissible use of the Special Services. End User recognizes that INOVALON will suffer irreparable harm, and that monetary damages may be incalculable and/or inadequate in the event that End User retains data provided through the Special Services in breach of this Addendum, and therefore, such breach shall be entitled to remedy by injunctive relief, in addition to any and all other relief which may be available at law or at equity.

6.8. NEITHER END USER NOR INOVALON SHALL BE LIABLE TO THE OTHER FOR ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS ADDENDUM BROUGHT MORE THAN TWO (2) YEARS AFTER THE CAUSE OF ACTION HAS ACCRUED.

6.9. End User hereby designates the individual whose name, work address, email address and telephone contact information are set forth in the Order Form relating to this Addendum as its point of contact for all matters arising under this Addendum.

6.10. The following provisions of this Addendum shall survive the expiration or termination hereof: Sections 1, 2, 3, 4.1, 4.2, 4.4, 4.5, 5.1, 5.2, 6.1, 6.2, 6.6, 6.7, 6.8, 6.10 and 6.11.

6.11. Neither party shall be liable to the other for any act, failure to perform, delay in performance, event or circumstance under this Addendum if, and to the extent, such act, failure to perform, delay in performance, event or circumstance is caused by conditions beyond its reasonable control and which, by the exercise of reasonable diligence, the delayed party is unable to prevent or provide against. Such conditions include, but are not limited to, acts of God; strikes, boycotts or other concerted acts of workmen; laws, regulations or other orders of public authorities; military action, state of war or other national emergency; fire or flood. The party affected by any such force majeure event or occurrence shall give the other party written notice of said event or occurrence within five (5) business days of such event or occurrence.

Annex 1 – End User Identity Verification

If End User is a public company or a health care provider, please provide the following information:

Public Company: A link to your company's filings on the SEC Edgar Database.

Health Care Provider: A link to one or more of the following web sites that document that the End User's address is an exact match to the listing found in any of the following: Medicaid or Medicare website, Joint Commission (www.jointcommission.org), Accreditation Association for Ambulatory Healthcare (AAAHC), Accreditation Commission for HealthCare (ACHC), American Association for Accreditation of Ambulatory Surgery Facilities (AAAASF), American Osteopathic Healthcare Facilities Accreditation Program (AOA/HFAP), Community Health Accreditation Program (CHAP), or Billian's HealthData. Alternatively, evidence that End User is an approved provider by a recognized, verifiable, medical health insurance carrier and the insurance carrier confirms that the End User resides at the same exact location listed on the relevant Order Form, or (1) a specific healthcare trade association (such as the American Dental Association); and (2) a current copy of a utility (electric or gas only) bill demonstrates an exact match on the address the End User conducts business from and the address where the utility company referenced reads a meter.

In addition, provide the following information:

- Description of End User's business and the reason for obtaining the Special Services.
- Organization Certificate or other evidence of legal entity status and existence.
- Copy of business license(s), if any.
- Bank relationship and credit references.
- For non-profit institutions, a copy of the letter granting tax exemption from the Internal Revenue Service.

Annex 2 – CRA Information Security Safeguards -- End User Authentication

To the extent that an End User obtains either directly from CRA, or through INOVALON, any of the following, it shall comply with the following requirements:

- The CRA -issued subscriber codes and passwords must be protected from unauthorized use and End User may not furnish them to any third party.
- CRA -issued subscriber passwords must be changed if there has been any actual or suspected compromise or misuse of the passwords

- End User must use strong authentication mechanisms to protect against delivery of CRA Data to unauthorized individuals

- The authentication process must identify the individual who obtains the report at the End User's location. Authentication at the company level is not adequate.

- If identification codes ("IDs") and passwords are being used for authentication:

- Strong password policies must be in place (minimum length of 8 alpha and numeric characters, frequent and mandatory password changes – at least every ninety (90) days)

- IDs and passwords must be encrypted with strong (at least 128-bit) encryption keys when they travel over the Internet

- If digital certificates are used for individual authentication, the certificate authority must be trusted, the certification process must be sound, and the certificate must be protected by the end user. (NOTE: If both digital certificates and IDs/passwords are being used, the 90-day password change requirement is not required as long as the certificates are renewed no less frequently than on an annual basis)

- Servers storing IDs and passwords and/or digital certificate information must be secured with the same security measures as the servers holding CRA Data

- End user must promptly disable or inactivate IDs or digital certificates of individual users who are no longer authorized to obtain CRA Data

The End User's application must have adequate audit trails and detailed reports that allow early detection of fraudulent access and/or investigation of suspicious activity.

The application must have a timeout feature so that the End User must re-authenticate after an extended period of inactivity. The recommended setting for the timeout is thirty (30) minutes

Individual End User IDs and passwords must not be pre-installed, electronically "remembered," or scripted.

End User is responsible for protecting its passwords and for protecting confidential CRA Data that may be on its workstations.

End User is encouraged, but not required, unless by law, to encrypt, mask or truncate social security numbers and/or account numbers.

A third-party review by recognized security professionals of the End User's security measures is highly recommended.

Annex 3 – CFPB's Notice to Users of Consumer Reports: Obligations of Users under the FCRA

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 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 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. Section 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 or 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 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 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 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 the 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 subject 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 below.
- Upon 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 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 as 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. Section 603(l), 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 to 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. This statement must include the address and the toll-free telephone number of the appropriate notification system.

In addition, once the CFPB 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 as to 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 the FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:

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