September 1, 2021

MASTER SERVICES AGREEMENT--TERMS AND CONDITIONS

This National Credit Center Master Service Agreement (the “Master Agreement”), governs the service documents identified below. This Master Agreement and other service documents listed below are collectively referred to as the “Service Documents”.

The Service Documents described below contain the terms under which National Credit Center LLC, to include but not limited to, affiliates, subsidiaries and other business ventures (“NCC”), will provide services pursuant to the National Credit Center Service Order Agreement (“Service Order”), which may include other specified services and collectively referred to as the “Services” provided.

The NCC customer to which NCC will provide Services, is the signatory specifically identified to receive Services on the Service Order Agreement that includes but not limited to its affiliates, subsidiaries and other business ventures (“Client”). NCC and Client maybe referred to individually as a “Party” or collectively as the “Parties”.

NCC and Client agree:

1. **Service Documents.**

The Service Documents, negotiated and modified by NCC and Client, include but not limited to, the individually named documents below:

A. National Credit Center Master Agreement (“Master Agreement”)

a. Exhibit 1 A – Information Security Requirements

b. Exhibit 1 B – Required Compliance, Terms and Conditions

B. National Credit Center Service Order Agreement (“Service Order”)

a. Exhibit 1 – Client Business Information

b. Exhibit 2 – Service Order Form

2. **Services.**

NCC and Client will agree to the specific Services(s) to be provided, as identified in the Service Order and any other related documents that specifically references and incorporates by reference this Master Agreement.

3. Sole and Exclusive Provider.

NCC shall be the sole and exclusive provider to the Client of credit reports and products provided through Experian, Equifax and Transunion.

4. **Document Modification.**

The Service Documents, from time to time, may be modified in writing without prior written notice to Client or any other party, unless specifically referenced in the Service Order or other related document. The most current version of this Master Agreement is available for review at nccdirect.com and is binding.

5. **Fees, Payment, Late Payment Resolution Process.**

Client agrees to pay for Services pursuant to the Service Order which is subject to

increase without prior notice.

A. Invoice and Payment

For services rendered, NCC will invoice Client monthly or as specified on the applicable Service Order. Upon receipt, Client agrees to immediately pay each invoice in full in available U.S. Dollars via ACH, bank check or via credit card without setoff, counterclaim, discount, abatement or demand.

Invoices will be sent to the address indicated on the applicable Service Order or other related document that indicates the Client's billing address.

B. Late Payment and other Charges

Any invoice not properly disputed as provided in section 5(C) below and not paid in-full by the due date stated on the invoice ("Due Date"), shall be subject to a late payment charge of one and one-half percent (1.5%) or twenty-five dollars ($25.00) per credit bureau report, service and or solution, whichever is greater, per month on the delinquent account balance until paid in full.

NCC reserves the right to assess a $25 fee for any check returned for insufficient funds or not paid when presented for payment.

C. Payment Disputes Process

(i) The Parties agree to use good faith efforts to resolve any payment dispute. All payment disputes must be claimed within ninety (90) days after the Due Date or the claim is barred unless manifest error.

(ii) In good faith, Client may dispute in writing the amount or appropriateness of any invoiced fee or other charge as follows: Client shall provide a written notification to NCC at *ncccustomersupport@nccdirect.com* of the fee(s) or other charge(s) being disputed

along with substantiating documentation and other information reasonably requested by NCC to resolve the payment dispute (“Payment Dispute Process”).

(iii) If agreed by NCC and Client, Client shall remain responsible by the Due Date for the invoiced amount excluding the disputed amount.

(iv) Absent manifest error, failure to contest fee(s) or charge(s) pursuant to the Payment Dispute Process shall create an irrefutable presumption of correctness of the fee(s) or charge(s), and Client shall be deemed to have waived its dispute rights for the applicable invoice and agreed to pay such invoice in full.

6. **Confidentiality of Information.**

A. The term “Confidential Information”, includes but is not limited to, all information, including Bureau Data, intellectual property owned or licensed to Client by NCC, documents, agreements, files, whether transferred verbally or electronically or written or any other media format whether observed or stored, all consumer, client and customer information, any personally identifiable information, as well as proprietary information such as – trade secrets, know how, processes, methods, practices, analyses, compilations, documents that reflect or are generated from such information, documents or any other materials to the extent disclosed concerning the business and affairs of NCC.

B. Nothing contained in the Service Documents grants or alters any property rights, by license, ownership or otherwise, to Client of any Confidential Information of NCC or its service providers. Confidential Information shall and will remain the sole and exclusive property of NCC.

C. Client agrees that Confidential Information shall not be reproduced in any form except in conjunction with accomplishing the Services contracted.

D. Except as provided for in the Service Documents, Client shall not make any disclosure of Confidential Information to anyone other than those individuals, agents and employees that need to know (“Authorized Persons”) in order to accomplish the duties and obligations under the Service Documents. Client shall make all Authorized Persons aware and responsible for the terms and conditions of controlling NCC’s Confidential Information.

E. Client agrees to follow the required security information protocols of the appropriate Credit Bureau as described in the exhibits attached to this Master Agreement, which may be updated from time to time. Further, Client agrees that Confidential Information received in any form or via any medium shall: (a) be stored in a physically and logically secure and controlled environment, only accessible by Authorized Persons; and (b) be downloaded only onto physically and logically secured and controlled systems accessible by Authorized Persons.

F. Upon written request by NCC, Client shall promptly return to NCC or securely destroy, all Confidential Information and all copies thereof. Confidential Information disposed of in the regular course of business shall be securely destroyed on a regular basis. Notwithstanding, Client may retain copies of any Confidential Information required to comply with applicable law or regulation provided (i) such information shall remain subject to this Master Agreement and (ii) shall not be retained beyond the period required by applicable law or regulation.

G. Client acknowledges and agrees that an actual or threatened breach of any of the terms and or conditions contained in this section will result in irreparable and continuing damage to NCC for which there will be no adequate remedy at law, and NCC shall be entitled without the requirement of posting a bond or other security, to injunctive relief, specific performance and or other equitable relief as remedies for such breach or threatened breach, and other relief as may be proper (including monetary damages if appropriate), and these remedies shall not be deemed NCC's exclusive remedies but shall be in addition to all other remedies available at law or in equity to NCC.

7. **Term, Suspension and Termination.**

A. Term

A Service Order shall remain in effect for three (3) years ("Initial Service Term") and shall automatically renew for consecutive three (3) year terms ("Renewal Term"), unless terminated sooner in accordance with the Service Order and/or other Service Documents.

B. Suspension

NCC reserves the right, in its sole and exclusive discretion and without liability, to suspend Services to Client for any Default as described in this section below.

C. Termination

(i) Client may terminate the Renewal Term and related Service Order after giving notice to NCC pursuant to §10 below sixty (60) days prior to the Renewal Term.

(ii) After giving reasonably written notice to Client and without any liability to NCC, NCC may immediately terminate any and all Services to Client for a Default as described below.

(iii) Each of the following shall constitute an event of default ("Default") under this Agreement:

a) Client's failure to pay any invoice after the Due Date;

b) Client's failure to comply with any Federal or state law;

c) Client's failure to comply with any requirement of a credit provider, including but not limited to Equifax Information Services LLC, Transunion, Experian Information Solutions, Inc. or any of their affiliated companies ("Credit Bureau" or collectively the "Credit Bureaus");

d) If Client is seeking to become or has become a subject to any insolvency, bankruptcy proceeding, dissolution or cessation of business operations;

e) A Credit Bureau requests NCC to terminate service to Client;

f) Client breaches any term or condition of the Service Documents.

8. **Representations and Warranties.**

A. Client Represents and Warrants

Client represents and warrants that:

(i) Client will not use any Service in a manner that could result in a contravention of Federal or state law and NCC policy;

(ii) Client represents and warrants that it shall comply with all the requirements of the Credit Bureaus as outlined in the attached exhibits;

(iii) Client represents and warrants that it shall comply with all applicable laws, regulations and ordinances and shall maintain in effect all the licenses, permissions, authorizations, consents and permits that it needs to carry out its obligations under the Service Documents;

(iv) Client represents and warrants that its employees and agents that use or have access to any Service are duly authorized with the appropriate authority to act and Client will exercise appropriate controls to ensure each employee and agent does not exceed the authority granted and abide by security protocols, procedures and policies consistent with maintaining Confidential Information;

(v) Client represents and warrants that it shall establish and enforce appropriate security protocols, procedures and policies consistent with maintaining Confidential Information and Credit Bureau requirements. Client represents and warrants that it shall be the end user for all information received from NCC.

(vi) Client represents and warrants that it will use all information received from NCC for a permissible purpose and abide by other obligations as stated and described by 15 U.S.C. §1681et al of the Fair Credit Reporting Act (FCRA) and GLBA.

(vii) Client represents and warrants that it will not endeavor in a business not served or prohibited by the Credit Bureaus and/or Federal or State law, and will abide by the

information security and other requirements of the Credit Bureaus as described in the exhibits entitled “Information Security Requirements” and “Required Compliance, Terms and Conditions” which may be updated from time to time.

B. NCC Representations and Warranties

TO THE FULLEST EXTENT PERMITTED BY LAW, NEITHER NCC NOR THE CREDIT BUREAUS MAKE ANY WARRANTY OR REPRESENTATIONS WITH RESPECT TO THE SERVICE(S) PROVIDED BY NCC UNDER ANY AND ALL OF THE SERVICE DOCUMENTS AND EXPRESSLY DISCLAIM ANY AND ALL REPRESENTATIONS AND WARRANTIES WRITTEN, ORAL, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANT ABILITY, INFRINGEMENT, COMPLETENESS, QUALITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE. NEITHER NCC NOR THE CREDIT BUREAUS REPRESENT OR WARRANT THAT THE SERVICE(S) PROVIDED WILL BE UNINTERRUPTED, FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS OR ERROR FREE. ANY REPRESENTATION OR WARRANTY EXPRESSLY SET FORTH IN A SERVICE ORDER CONSTITUTES THE ONLY REPRESENTATION OR WARRANTY OF NCC AND RELATES SOLELY TO THE SPECIFIC SERVICE ORDER. NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED HEREIN, UNDER NO CIRCUMSTANCES WILL NCC OR THE CREDIT BUREAUS HAVE ANY LIABILITY FOR INTERRUPTIONS AFFECTING THE SERVICES FURNISHED UNDER THIS AGREEMENT THAT ARE ATTRIBUTABLE TO CLIENT’S EQUIPMENT FAILURE, OR CLIENT’S BREACH OF THE AGREEMENT, OR FOR ANY ACT OR OMISSION OF A THIRD PARTY PROVIDING ANY SERVICE OR PRODUCT THAT IMPACTS THE SERVICE(S) PROVIDED UNDER THE SERVICE DOCUMENTS. THE PARTIES ARE COMMERCIAL ENTERPRISES, CLIENT HAS THE UNDERSTANDING AND COMPREHENSION OF THIS SECTION AND THE OPPORTUNITY FOR REVIEW BY LEGAL COUNSEL.

9. **Limitation of Liability and Indemnification.**

A. Limitation of Liability

The liability of NCC arising out of or in connection with the Services Documents, shall not exceed the amount of fees actually collected by NCC from Client during the previous twelve (12) months before the incident that gave rise to the claim. In no event shall NCC or the Credit Bureaus be liable for indirect, special, punitive incidental or consequential damages of any kind, including but not limited to profits, actual or projected revenues, business harm, regardless if the action is based on warranty, strict liability, tort, negligence of any kind, nonperformance, termination, action or inaction for any reason even if Client advises of the possibility of such loss or damage. Client agrees that this limitation set forth in this section is integral to the charges for Services and if NCC were to assume any further liability than set forth herein, said Services charges would of necessity be substantially higher. The Parties are commercial

enterprises, Client has the understanding and comprehension of this section and the opportunity for review by legal counsel.

B. Indemnification

Client agrees to indemnify and hold NCC and its directors, officers, employees and agents and the Credit Bureaus harmless from all claims, demands, losses, liabilities, judgments and expenses (including their attorneys' fees and legal expenses) arising out of or in any way connected with NCC's performance, breach or failure of express or implied warranty, gross negligence, even if informed by an authorized agent or negligence of any kind under the Service Documents. The Parties are commercial enterprises, Client has the understanding and comprehension of this section and the opportunity for review by legal counsel.

10. **Notice.**

Any and all notices, demands or requests required or permitted to be given under the Service Documents shall be given in writing and sent, by registered or certified U.S. mail, return receipt or by overnight courier with a confirmation of delivery tracking system, addressed to the other Party hereto at its address set forth in the Service Documents, in particular, the Service Order. Each Party may from time-to-time change the address for notice by giving the other party written notice in accordance with the terms of this section.

A. Notices to NCC shall be sent to the attention of:

National Credit Center

Mike Sabin, CEO

7373 Peak Dr #250

Las Vegas, NV 89128

B. Notice to Client shall be addressed as indicated on the Service Order.

11. **Arbitration and Waiver of Jury Trial.**

A. Arbitration

The Parties agree in the event a dispute arises concerning the Service Documents, whereby the value of the claim is less than ten-thousand dollars ($10,000), litigation will not afford a practical resolution of the issues within a reasonable period of time and at a reasonable cost. Consequently, any claim less than ten-thousand dollars ($10,000),with the exceptions noted below, each Party agrees that any dispute, controversy or claim arising out of or relating to this contract, including the formation, interpretation, breach

or termination thereof, including whether the claims asserted are arbitrable, will be referred to and finally determined by binding arbitration in accordance with the JAMS International Arbitration Rules. The tribunal will consist of a sole arbitrator. The seat of the arbitration will be located in Las Vegas, Clark County, Nevada. The language to be used in the arbitral proceedings will be American English. The arbitrator shall award the prevailing party fees and costs. Judgment upon the award rendered by the arbitrator may be entered by any court having jurisdiction thereof. The losing party shall pay the filing and arbitrator's cost, if any, of the successful party. For purposes of this provision, the following matters will not be subject to arbitration, matters relating to the breach of Confidential Information, which NCC may seek to enforce in any court of competent jurisdiction. Either Party may initiate an arbitration proceeding at any time by giving notice to the other Party. The arbitration proceeding and all filing, testimony, documents, and information, relating to or presented during the proceeding, shall be disclosed exclusively for the purpose of facilitating the arbitration process and for no other purpose and shall be deemed to be information subject to section 7, Confidential Information, of this Master Agreement. The decision of the arbitrator, absent fraud, duress, incompetence or gross and obvious error of fact, shall be final and binding upon the Parties and shall be enforceable in courts of proper jurisdiction. Following written notice pursuant to section 10, of a request for arbitration, each Party shall be entitled to an injunction restraining all further proceedings in any pending or subsequently filed litigation concerning the Service Documents, except as otherwise provided herein.

B. Waiver of Jury Trial

Each Party acknowledges a controversy that may arise under the Service Documents are likely to involve complicated and difficult issues, therefore, each Party irrevocably and unconditionally waives any right to a trial by jury in respect of any legal action arising out of or relating to the Service Documents.

12. **Governing Law and Venue, No Waiver of Remedy, Attorney Fees.**

A. Governing Law and Venue

The Service Documents are governed by and to be construed in accordance with the laws of the State of Nevada, without regard to conflict of laws, rules and without regard to provisions related to the choice of law or forum. Unless strictly prohibited by applicable law, any action brought to enforce the terms of the Service Documents shall be brought in the Federal and State Courts of Clark County, Nevada.

B. No Waiver of Remedy

Except as otherwise set forth in the Service Documents, no failure to exercise, or delay in exercising, any right, remedy, power or privilege arising from any of the Service Documents shall operate or be construed as a waiver thereof, nor shall any single or partial exercise of any right, remedy, power or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power or privilege.

C. Attorney Fees

In the unlikely event a Party seeks enforcement of or defended against an unsuccessful claim of breach of the Service Documents, the unsuccessful party shall be liable for all reasonable attorney fees, expenses and costs incurred by the successful party.

13. **Miscellaneous.**

A. Independent Entities

The Service Documents shall establish no relationship between the Parties other than that of an independent contractor. Neither Party's employees or agents shall be construed to be a representative of the other Party. None of the provisions of the Service Documents are

intended to create, nor shall they be deemed or construed to create, any partnership, joint venture or other relationship between the Parties other than that of independent contracting parties.

B. Taxes and Other Exemptions

(i) Client shall be responsible for all charges, including but not limited to, fees, taxes, regulatory fees, governmental assessments, surcharges, value added tax, and other charges imposed on Client as a result of NCC's sale of Services or Client's use of Services during the course of business. NCC shall not be responsible in any manner, under any conditions or in any terms liable or responsible for the above referenced charges.

(ii) If Client claims a tax exemption of any kind, Client must provide evidence of such exemption to NCC that is satisfactory to NCC in NCC's sole and absolute discretion. NCC may invoice Client for all charges NCC deems, in its sole and absolute discretion, not covered by the Client's exemption and Client shall promptly pay such invoice by the Due Date without setoff, counterclaim, discount, abatement or demand. Any outstanding balance shall remain Client's sole and absolute responsibility.

C. Assignment or Delegation

Neither Party may assign, delegate or transfer its rights or obligations under the Service Documents without the other Party's prior written consent, which consent may not be unreasonably delayed or withheld, however, no such consent will be required by NCC if such assignment or delegation is to an affiliate or successor-in-interest (by merger, acquisition, asset sale, or otherwise). Except as provided herein, any assignment or delegation without prior written consent from the other Party is null and void.

D. No Third-Party Beneficiaries

Nothing in the Service Documents shall be construed to create any rights or obligations except between the Parties hereto, and no person or entity shall be regarded as a third-party beneficiary under the Service Documents. NCC and the Credit Bureaus shall be entitled to inspect and audit records and files of Client as it relates to the Services provided.

E. Force Majeure

NCC will not be liable for delays in its performance or failure to perform in whole or in part of the terms of the Service Documents caused by the occurrence of any contingency beyond its control, including but not limited to, labor dispute, strike, labor shortage, shortage of supplies or materials, vendor issues, war or act of war, insurrection, sabotage, riot or civil commotion, act of a public enemy, epidemic, accident, fire, Credit Bureau nonperformance, storm, earthquake, explosion, flood, drought or other act of God, act of any governmental authority, judicial action, equipment failure, outage or technical failure, electrical outage and any such delay or failure will not be considered a breach of the Service Documents.

F. Severability

The invalidity or unenforceability of any term or provision contained in the Service Documents shall not void or impair the remaining provisions hereof, which shall remain in full force and effect as if such invalid or unenforceable provision had never been contained herein.

G. Construction and Headings

In the event of an ambiguity or if a question of intent or interpretation arises, the Service Documents shall be construed as if drafted jointly by the Parties and no presumption or burden of proof shall arise favoring or disfavoring any Party by virtue of the authorship of any of the provisions. The section headings contained herein are for reference purposes only and shall not affect in any way the meaning or interpretation of the Service Documents.

H. Entire Agreement

The Service Documents constitutes and represents the entire agreement between Parties regarding the Services to be provided and supersedes and extinguishes all prior agreements, understandings, representations, warranties and arrangements of any nature, whether oral or written, but excludes any specifically drafted and agreed upon arrangement(s) by the Parties.

I. Survival

Notwithstanding anything herein to the contrary, sections 7, 8, 9, 11 and 12 shall survive after the termination all the Service Documents.

Exhibit 1 A

Information Security Requirements

The terms and conditions of this exhibit meets and/or exceeds the information security requirements of the three national credit reporting agencies (Equifax Information Services LLC, Transunion, Experian Information Solutions, Inc.), where applicable, complies with the access of information requirements of the Federal Fair Credit Reporting Act and Gramm-Leach-Bliley Act for data privacy (FCRA and GLB 5A Data). In addition, this exhibit complies with the notification requirements prescribed by the California Consumer Credit Reporting Agencies Act and the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999) § 2480e, as well as, the requirements of the Fair Isaac Company and affiliates (FICO).

1. **Definitions and Key Terms**

Credit Bureau and/or **Credit Bureaus** shall mean, individually or collectively, any of the three national credit reporting agencies (Equifax Information Services LLC, Transunion, Experian Information Solutions, Inc.).

Credit Bureau Data means any Consumer Report and/or any other related consumer information received by NCC and/or Client who has a permissible purpose for receiving such information in accordance with the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.) including, without limitation, all amendments thereto ("FCRA").

Client shall refer to the signatory specifically identified on the Service Order Agreement, includes but not limited to its affiliates, subsidiaries and other business ventures, to receive services.

Consumer Information refers to Consumer Reports and other non-public, personally identifiable consumer information obtained from the Credit Bureaus.

Consumer Report shall have the meaning set forth in the Fair Credit Reporting Act ("FCRA"), 15 USC 1681(a)(d), as may be amended from time to time. For purposes of this Exhibit, the term Consumer Reports refers to those consumer reports, or any information derived therefrom including, but not limited to scores, obtained from any of the Credit Bureaus.

Consumer Reporting Agency ("**CRA**") shall have the meaning set forth in the FCRA, 15 USC 1681 (a)(f), as may be amended from time to time. As of the date of this Exhibit, the term "Consumer Reporting Agency" is defined in the FCRA as an entity which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part-in the practice of assembling or evaluating consumer credit

information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

Death Master File (DMF) is made available by the U.S. Department of Commerce National Technical Information Service (NTIS) and subject to regulations found at 15 CFR Part 1110. All users are required to comply with all applicable laws with respect to DMF data.

Federal Fair Credit Reporting Act (FCRA) refers to the Federal Fair Credit Reporting Act, 15 USC 1681 et seq., as amended from time to time.

Exhibit 1 A-1

[Attached – ASR Security Requirements]

Fair Isaac Corporation (FICO) formally referred to as Fair Isaac and Company and any of the FICO scoring models.

Financial Modernization Act of 1999 (GLBA) refers to the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act or GLB Act.

Permissible Purpose – NCC and the Client certify that any Consumer Reports or related Credit Bureau Data will only be used for a permissible purpose and used for no other purpose other than prescribed by the Fair Credit Reporting Act ("FCRA").

Services refers to, but not limited to, the services specified on the NCC Service Order signed by the Client.

Service Order Agreement (Service Order) references to, but not limited to, the Services agreed to by Client as indicated on the executed Service Order and other related documents.

Subscriber Code is the code number (account number) assigned to NCC and Client to access Credit Bureau Data and systems.

1. Information Security Requirements

[Access Security Requirements]

1. General Requirements

1. Designate a contact

NCC will designate the primary contact for the Credit Bureaus as the Chief Compliance Officer [Scott Moody smoody@nccdirect.com or 877-709-7222] and SVP of Product [Jim Dietrich jdietrich@nccdirect.com or 877-709-7222].

2. NCC and Client certify

1. Credit Bureau Data will be used for a permissible purpose under Section 604 of the FCRA for the Consumer Reports.

2. NCC and Client are permitted to receive and use nonpublic personal information under Section (6802)(e) of GLBA.

3. NCC and Client are permitted to receive and use nonpublic personal information under Section (6802)(e) of GLBA for identification services that are sourced from databases other than the Credit Bureaus .

4. Client will permit NCC and Credit Bureau to inspect and audit its records and files as it relates to the Services provided by NCC and the Credit Bureaus.

5. Client will not resell Credit Bureau Data.

3. Businesses not served – Unauthorized Business Types

NCC will not sell Credit Bureau Data to a Client that is in any of the following categories and Client certifies they do not belong to, or intend to belong to, any of following categories or types of businesses:

1. Adult entertainment service of any kind

2. Asset location service

3. Attorney or Law Firm engaged in the practice of law, unless engaged in collection or using the report in connection with a consumer bankruptcy pursuant to the written authorization of the consumer.

4. Bail Bondsman, unless licensed by the state in which they are operating

5. Child location service (i.e. company that locates missing children)

6. Credit counseling, except not-for-profit consumer credit counseling companies

7. Credit repair clinic

8. Dating service

9. Financial counseling, except a registered securities broker dealer or a certified financial planner

10. Foreign company or agency of a foreign government

11. Genealogical or heir research firm

12. Law enforcement agency

13. Massage service

14. News agency or journalist

15. Pawn shop

16. Private detective, detective agency or investigative company

17. Repossession company

18. Subscriptions (magazines, book clubs, record clubs, etc.)

19. Tattoo service

20. Time Shares – Company seeking information in connection with time shares (exception:

financers of time shares)

21. Weapons dealer, seller or distributor

22. Other companies that resell Credit Bureau Data

4. Suspend and/or Termination of Services

As described in the Mater Agreement §6(C)(iii), NCC or the Credit Bureaus may suspend or terminate Client services for a Default which include but not limited to:

1. Client's failure to comply with any Federal or state law

2. Client's failure to comply with any requirement of a Credit Bureau

3. If Client is seeking to become or has become a subject to any insolvency, bankruptcy proceeding, dissolution or cessation of business operations

4. A Credit Bureau request NCC to terminate service to Client

5. Client breaches any term or condition of the Service Documents.

2. Specific Access Control Requirements for – NCC, Client and Third-Party

a. All user credentials such as Subscriber Code number, Subscriber Code passwords, User names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party.

b. If using third party or proprietary system to access Credit Bureau'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.).

c. If a third party or third-party software or proprietary system or software, used to access Credit Bureau Data or systems, is replaced or no longer in use, the passwords should be changed immediately.

d. A unique user ID for each user is to be created to enable individual authentication and accountability for access to Credit Bureau infrastructure. Each user of the system access software must also have a unique logon password.

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

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

g. Develop strong passwords that are:

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

h. Passwords (e.g. subscriber code passwords, user password) must be changed immediately when:

1. Any system access software is replaced by another system access software or is no longer used
2. The hardware on which the software resides is upgraded, changed or disposed
3. Any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements)

i. Ensure that passwords are not transmitted, displayed or stored in clear text; protect all NCC, Client and Third-Party (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 algorithms are utilized (e.g. AES 256 or above).

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

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

l. Ensure that personnel who have 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.

m. NCC, Client and Third-Party must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Credit Bureau Data.

n. Ensure that NCC, Client and Third-Party 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.

o. Implement and manage a process to terminate access rights immediately for users who access Credit Bureau Data or systems when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.

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

q. Implement and manage 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.

r. Implement and manage physical security controls to prevent unauthorized entry to NCC, Client and Third-Party 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.

s. Client and NCC certify that they will access, use and store Credit Bureau Data only within the territorial boundaries of the United States, Canada, and United States territories of Puerto Rico, Guam and the Virgin Islands.

3. Network Security and Data/Information Security Standards

On file and accessible to the Credit Bureaus upon request, NCC will maintain an updated and comprehensive Information Security Policy and an Acceptable Use Policy. NCC will install the necessary hardware and software to interface with Credit Bureaus. NCC will use the high standards of network and data security which is consistent with regulatory, legal and industry standards and incorporates the standards of:

a. ISO 27001/27002 standards of control
b. Credit bureau information and data security requirements (Equifax, Experian and Transunion)
c. Federal Finical Institute Examination Council - Information Technology Examination Handbook (FFIEC Examiners Guidelines)
d. National Institute of Standards and Technology (NIST)
e. Payment Card Industry Data Security Standard (PCI DSS)
f. GLB Safeguard Rules
g. FACTA Disposal Rules

NCC will maintain policies and procedures to address the following requirements:

a. Wireless Security
b. Network Security
c. Firewall Management
d. Use of Secure Protocols
e. Prohibition of Split Tunneling
f. Network Segmentation

NCC will keep current and maintain operating systems and infrastructure to industry best practices that include but not limited to: firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate patches that are no more than one version behind; as well as, updates, disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/ programs, while enabling the most secure configuration features to avoid unnecessary risks.

In addition, NCC will follow current best security practices for computer virus detection scanning services and procedures:

a. 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.

b. 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.

c. If NCC or Client suspects 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.

Further, NCC will encrypt Credit Bureau Data above AES 256 when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers and/or databases. When accessing Credit Bureau Data on devices such as smart tablets or smart phones the devices will be protected via a pass-code. NCC uses a VPN to protect data while in transmission. When no longer in use, electronic media containing Credit Bureau 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).

NCC will maintain policies and procedures to address the following physical and environmental security concerns:

a. Physical Access Restrictions
b. Visitor Access Requirements
c. CCTV Monitoring
d. CCTV Video Retention
e. CCTV logs must be maintained for 90 days online and 1 year archived.
. Clean Desk / Clear Screen
g. Climate Control System Monitoring:
h. Heat, Smoke, Fluid, Water Detection
i. Fire Suppression
j. Generator and Uninterruptable Power Supplies (UPS) Visitors must be escorted at all times where Information Assets are processed, stored, or transmitted.

4. Mobile and Cloud Technology

NCC will not store Credit Bureau Data on mobile devices. Any exceptions will be obtained from the specifically effected Credit Bureau.

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.

a. 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.

b. 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.

c. 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 Credit Bureau Data to be exchanged between secured and nonsecured applications on the mobile device.

d. In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Credit Bureau Data via mobile applications (internally developed or using a third-party application), ensure that multi-factor authentication and/or adaptive/ riskbased authentication mechanisms are utilized to authenticate users to application.

e. When using cloud providers to access, transmit, store, or process Credit Bureau Data ensure that:

1. Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations

2. 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 the Credit Bureaus:

(i) ISO 27001
(ii) PCI DSS
(iii) EI3PA
(iv) SSAE16 – SOC2 or SOC 3
(v) FISMA
(vi) CAI/CCM assessment

5. Data Breach

If it is believed that Credit Bureau Data is compromised, the specific Credit Bureau will be notified within twenty-four (24) hours or as otherwise required per contractual agreement and the proper notification procedure shall be followed by NCC according the effected Credit Bureau's reseller guidelines.

6. Regularly Monitor and Test Networks

Per NCC's Information Security Policy, NCC will 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.). Logs will be maintained for 90 days online and 1 year archived.

Audit trails will be enabled and active for systems and applications used to access, store, process, or transmit Credit Bureau Data establish a process for linking all access to such systems and applications.

Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Credit Bureau 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:

a. Protecting against intrusions
b. Securing the computer systems and network devices
c. Protecting against intrusions of operating systems or software.

2. Death Master File

Death Master File (DMF) is made available by the U.S. Department of Commerce National Technical Information Service (NTIS) and subject to regulations found at 15 CFR Part 1110. All users are required to comply with all applicable laws with respect to DMF data.

Client acknowledges that many services containing Experian information also contain information from the Death Master File as issued by the Social Security Administration ("DMF"); certify pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102 that, consistent with its applicable FCRA or GLB use of Experian information, the client's use of deceased flags or other indicia within the Experian information is restricted to legitimate fraud prevention or business purposes in compliance with applicable laws, rules regulations, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1); and certify that the client will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian information

3. Unauthorized Business Types

Not An Unauthorized Business Types
Client certified, warrants and represents that it is not engaged in nor will it engage in any of the following business during the term of this Service Order: (i) adult entertainment; (ii) business operating out of an apartment or residence; (iii) attorney or law office; (iv) bail bonds services; (v) check cashing services; (vi) credit counseling or credit repair; (vii) dating service; (viii) financial counseling; (ix) genealogical or family heir research services; (x) massage services; (xi) missing children location services; (xii) pawn shop; (xiii) detective services; (xiv) any individual wishing to perform investigations for private use; (xv) third party repossession services; (xvi) spiritual counseling services; (xvii) subscription services; (xviii) tattoo services; (xix) time share services; (xx) insurance claims. Client further represents and warrants that it is familiar with and will comply with all applicable consumer financial protection laws, all applicable requirements of the Fair Credit Reporting Act ("FCRA"), 15 USC Section1681 et seq., the Federal Equal Credit Opportunity Act, the Gramm-Leach-Bliley Act and any amendments to them, all state law counterparts of them, all applicable regulations promulgated under any of them including, without limitation, any provisions requiring adverse action notification to the consumer. In addition, Client shall not engage in any unfair, deceptive, or abusive acts or practices.

4. FCRA Permissible Purpose and GLB Appropriate Use

FCRA Permissible Purpose and/or GLB Appropriate Use

(i) Client certifies, represents and warrants to NCC that it has a permissible purpose for obtaining Consumer Reports in accordance with the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.) including, without limitation, all amendments thereto. Client will only use Gramm-Leach Bliley Act information for fraud prevention products.

(ii) Client shall use the Consumer Reports only for (a) its exclusive use and (b) solely for its one time use and for the purpose(s) of (1) pre-screening applicants for credit; and/or (2) 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. Client certifies that it will only request Consumer Reports for the permissible purpose(s) certified above and for Client's exclusive authorized use. Client further certifies and agrees that all Consumer Reports requested will be held in strict confidence pursuit to section 7 of the Master Agreement, except to the extent that disclosure to others is required or permitted by applicable law. Only designated and authorized representatives of Client will request Consumer Reports on behalf of Client. Client shall prohibit its employees from obtaining Consumer Reports on themselves, associates or any other persons except in the exercise of their official duties. Client will not disclose information from Consumer Reports to the subject of the report or any third party except as permitted herein or required by law, but will refer the subject of the Consumer Report to the applicable Credit Bureau. Client agrees to implement appropriate procedures so that only employees with adequate training regarding the requirements of the FCRA and other applicable law have access to Consumer Reports.

[FICO Addendum]
5. Required Compliance, Terms and Conditions

1. FRCA Compliance

As a user of Consumer Reports, NCC and Client will comply with all applicable FCRA regulations currently in effect which can be currently found at the Consumer Financial Protection Bureau's website http://www.consumerfinance.gov/learnmore.

2. FICO Scoring Certifications

NCC and Client hereby understands and agrees to the following terms and conditions regarding the use of Consumer Reports and reason codes obtained through NCC and the Credit Bureaus:

1. Client may disclose the Consumer Reports provided to Client to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only.

2. Client agrees to comply with all applicable law and regulations with respect to use of the Consumer Reports and reason codes purchased from NCC and certifies that it has permissible purpose under the FCRA to obtain said Consumer Reports. Client agrees to limit its use of the Consumer Reports and reason codes to its own business and will not sell, transfer, license or distribute Consumer Reports or reason codes to third parties. Client agrees to maintain security procedures to minimize the risk of disclosure of Consumer Reports to employees without a legitimate need to know.

3. Client will not permit its employees, agents or subcontractors to use any of the trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of Equifax Information Services LLC, Transunion, Experian Information Solutions, Inc., Fair Isaac and Company, or the Affiliates of either of them, or of any other party involved in the provision of the Credit Bureau/Fair Isaac Model, without such entity's prior written consent.

4. Client will not permit its employees, agents or subcontractors to, in any manner, directly or indirectly, discover or reverse engineer (or attempt to discover or reverse engineer) any confidential and proprietary criteria developed or used by Credit Bureau/Fair Isaac in performing the Credit Bureau/Fair Isaac Model.

The Credit Bureau/Fair Isaac has warranted to NCC that the Credit Bureau/Fair, Isaac Model is empirically derived and demonstrably and statistically sound and that to the extent the population to which the Credit Bureau/Fair Isaac Model is applied is similar to the population sample on which the Credit Bureau/Fair Isaac Model was developed. The Credit Bureau/Fair Isaac Model score may be relied upon by Client to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to Client. Credit Bureau/Fair Isaac has further warranted to NCC that so long as it provides the Credit Bureau/Fair Isaac Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC Section 1691 et seq. The foregoing warranties are the only warranties Credit Bureau/Fair Isaac have given NCC with respect to the Credit Bureau/Fair Isaac model and such warranties are in lieu of all other warranties, express or implied, Credit Bureau/Fair Isaac might have given NCC with respect thereto, including, for example, warranties of merchantability and fitness for a particular purpose. NCC and each respective Client's rights under the warranty are expressly conditioned upon each respective Client's periodic revalidation of the Credit Bureau/Fair Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 et seq.).

3. Terms Applicable to FICO® Scores Additional

In addition to the terms and conditions - Client of credit risk scores of Fair Isaac Corporation ("FICO Scores") agree to the following:

From time to time, Client may request that Equifax provide FICO Scores, for, in each case, one of the following internal decisioning purposes requested: (a) in connection with the review of a consumer report it is obtaining from Equifax; (b) for the review of the portion of its own open accounts and/or closed accounts with balances owing that it designates; (c) 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; (d) for use as a selection criteria to deliver a list of names to Client, or Client's designated third party processor agent; (e) for transactions not initiated by the consumer for the extension of a firm offer of credit or insurance; or (f) with respect to the insurance risk scores only for use in connection with the underwriting of insurance involving the consumer. Client shall use each such FICO Score only once and, with respect to FICO Scores, only in accordance with the permissible purpose under the FCRA for which Client obtained the FICO Score.

Client acknowledges that the FICO Scores are proprietary and that Fair Isaac retains all its intellectual property rights in the FICO Scores and the Models (defined below) used by Equifax to generate the FICO Scores. Fair Isaac grants to Client, effective during the term of the Client agreement, a personal, nonexclusive, non-transferable, limited license to use, internally, the FICO Scores solely for the particular purpose set forth in Section 1 above for which the FICO Scores were obtained, including, but not limited to the single use restrictions set forth above. Client's use of the FICO Scores must comply at all times with applicable federal, state and local law and regulations, and Client hereby certifies that it will use each FICO Score only for a permissible purpose under the FCRA. Client shall not attempt to discover or reverse engineer the FICO Scores, Models or other proprietary information of Fair Isaac, or use the FICO Scores in any manner not permitted, including, without limitation, for resale to third parties, model development, model validation (except as expressly set forth above with respect to Archive Scores), model benchmarking, or model calibration. "Model" means Fair Isaac's proprietary scoring algorithm(s) embodied in its proprietary scoring software delivered to and operated by Equifax.

Client shall not disclose the FICO Scores nor the results of any validations or other reports derived from the FICO Scores to any third party (other than to a consumer as expressly permitted in the Service Order and this Section 3) unless: (a) such disclosure is clearly required by law, (b) Fair Isaac and Equifax provide written consent in advance of such disclosure; and/or (c) such disclosure is to Client's designated third party processor agent; provided however that in either (i.e., (b) or (c) above) event, Client may make such disclosure (or in the event of (c), direct Equifax to deliver such lists, only after Client has entered into an agreement with the third party that (i) limits use of the FICO Scores to only the use permitted to Client hereunder, (ii) obligates the third party provider to otherwise comply with these terms, and (iii) names Fair Isaac as an intended third party beneficiary of such agreement with respect to the Models, FICO Scores, and other Fair Isaac intellectual property and with fully enforceable rights. Client shall not disclose a FICO Score to the consumer to which it pertains unless such disclosure is (i) approved in writing by Fair Isaac or (ii) required by law or is in connection with adverse action (as defined by the FCRA) and then only when accompanied by the corresponding reason codes.

Fair Isaac represents and warrants that the scoring algorithm (s) used in the Models to produce FICO Scores are empirically derived and demonstrably and statistically sound; provided, that, this warranty is conditioned on (i) an Client's use of each FICO Score for the purposes for which the respective Model was designed , as applied to the United States population used to develop the scoring algorithm, (ii) the Client' compliance with all applicable laws and regulations pertaining to the use of the FICO Scores, including the Client's duty (if any) to validate or revalidate the use of credit scoring systems under the ECOA and Regulation B, and (iii) the Client's use of the FICO Scores otherwise remaining in compliance with the terms of the Service Order and this Exhibit with respect to FICO Scores. FAIR ISAAC AND EQUIFAX HEREBY DISCLAIM ALL OTHER WARRANTIES, WHETER STATUTORY, EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND OTHER WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE. IN NO EVENT SHALL EQUIFAX OR FAIR ISAAC BE LIABLE FOR ANY CONSEQUENTIAL, INCEDENTAL, SPECIAL, OR PUNITIVE DAMAGES INCURRED BY ANY PARTY AND ARISING OUT OF THE PERFORMANCE HEREUNDER, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF SUCH DAMAGES WERE REASONABLY FORESEEABLE. IN NO EVENT SHALL EQUIFAX'S AND FAIR ISAACS'S COMBINED AGGREGATE TOTAL LIABILITY HEREUNDER EXCEED THE AMOUNTS PAID HEREUNDER DURING THE PRECEDING TWELVE (12) MONTHS FOR THE FICO SCORES THAT ARE THE SUBJECT OF THE CLAIM(S) OR TEN THOUSAND DOLLARS ($10,000.00), WHICHEVER AMOUNT IS LESS.

Equifax and Client acknowledge and agree that Fair Isaac is a third party beneficiary hereunder with respect to the Model, FICO Scores, and other Fair Isaac intellectual property and with fully enforceable rights. Client further acknowledges and agrees that Fair Isaac's rights with respect to the Models, FICO Scores, other Fair Isaac intellectual property, and all works derived therefrom are unconditional rights that shall survive the termination for any reason.

4. FICO® Risk Score, Classic, V8, V8F, Auto Score, v5 F – is a credit scoring service based on a model developed by Fair Isaac Corporation ("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.

5. ACROFILE and ACROFILE Plus-- are the core consumer reports from the Equifax consumer credit database, consisting of identification information, credit file inquiries, public record information and credit account trade lines of the subject of the report. Client may access these credit reports on an individual basis or through Joint Files AccessSM, which provides simultaneous access to the credit files of both husband and wife with a single inquiry.

6. VantageScore Requirements

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 Client's receipt and use of VantageScore:

Client will request VantageScores only for Client's exclusive use. Client may store VantageScores solely for Client's own use in furtherance of Client's original purpose for obtaining the VantageScores. Client shall not use the VantageScores for model development or model calibration, except in compliance with the following conditions: (1) the VantageScores may only be used as an independent variable in custom models; (2) only the raw archived Score and Score segment identifier will be used in modeling (i.e. no other Score information including, but not limited to, adverse action reasons, documentation, or scorecards will be used); and (3) Client's depersonalized analytics and/or depersonalized third party modeling analytics performed on behalf of Client, using VantageScores, will be kept confidential and not disclosed to any third party other than as expressly provided for below in subsections (ii), (iii), (iv), (v) and/or (vi) of this paragraph. Client shall not reverse engineer the Score. 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, agents and independent contractors of Client with a need to know and in the course of their employment; (ii) to those third party processing agents and other contractors of Client who have executed an agreement that limits the use of the VantageScores by the third party only to the use permitted to Client and contains the prohibitions at least as restrictive as 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 VantageScore (provided that, accompanying reason codes are not required to the extent permitted by law); (iv) to government regulatory agencies; (v) to ratings agencies, dealers, investors and other third parties for the purpose of evaluating assets or investments (e.g. securities) containing or based on obligations of the consumers to which the VantageScores apply (e.g. mortgages, student loans, auto loans, credit cards), provided that, as it relates to this subsection (v), (a) Client may disclose VantageScores only in aggregated formats (e.g. averages and comparative groupings) that do not reveal individual VantageScores,

(b) Client shall not provide any information that would enable a recipient to identify the individuals to whom the VantageScores apply, and (c) Client shall enter into an agreement with each recipient that limits the use of the Score to evaluation of such assets or investments, or (vi) as required by law. Client agrees that the trademarks, trade names, product names, brands, logos, and service marks ("Vantage Marks") for VantageScores and VantageScore credit scoring models will remain the sole property of VantageScore Solutions, LLC. Client obtains a limited, nonexclusive, non-transferable, royalty free license to use and display the Vantage Marks in connection with the activities solely permitted by this Agreement. The use of the Vantage Marks under the preceding license is limited to use only in connection with the Services covered by this Agreement, and the Client expressly agrees not to use the Vantage Marks in connection with any products or services not covered by this Agreement. Any use of the Vantage Marks is subject to VantageScore Solutions, LLC's prior written authorization. Client further agrees it will include the Vantage Marks in all advertising and marketing materials which reference the VantageScores or Vantage models and it will comply with the VantageScore Trademark Policy and Brand Guidelines, which may be changed from time to time upon written notice. All use of the Vantage Marks will accrue solely to the benefit of VantageScore Solutions, LLC.

7. Equifax MLA Covered Borrower Status

Permissible use of the Equifax MLA Covered Borrower Status is limited to completing covered borrower checks pursuant to the Military Lending Act (MLA), as codified in 10 U.S.C. 5987.

8. Credit Bureau Identity and Fraud Services

Client certifies that it will use Credit Bureau identity and fraud services ("IFS Services") exclusively within Clients own organization for the purpose of verifying the identity of individual persons (ID Subjects) who initiates a business transaction with the Client and not for any other purpose; and that it will use and ensure that its employees access to the IFS Services is in accordance with the terms of the Client Agreement.

Client acknowledges and agrees that the IFS Services do not guarantee the identity of the ID Subject, but merely provide a risk assessment regarding the ID Subject's identity that is derived, in part, from information provided by the ID Subject or otherwise collected from an ID Subjects use of the IFS Services and relayed by Client to Credit Bureau ("ID Subject Content"); and that in connection with certain IFS Services; (i) Client will establish a risk decision threshold above which the ID Subject is verified or authenticated, depending on the applicable Service, and below which the ID Subject is not verified or authenticated ("Risk Decision Threshold") and Credit Bureau may act as a consultant to review Client's risk strategies, but Client, in its sole discretion, will set its Risk Decision Threshold(s); and (ii) that depending upon Client's Risk Decision Threshold an ID Subject may be able to successfully pass verification and authentication even though the individual submitting the ID Subject Content is not the actual individual to whom the ID Subject Content pertains.

Client shall not maintain, copy, capture, reproduce, re-use or otherwise retain in any manner the interactive questions or multiple choice answers provided as part of the IFS Services ("Queries"), the ID Subject responses to the Queries ("Answers") or the scores, flags and reason codes generated or other information relating to such Queries and Answers provided by the IFS Services (Scores); provided, however, that Client may capture and retain the unique transaction number generated by the IFS Services with each transaction (each a "Transaction ID" solely for the purpose of (i) audit trail; (ii) calculation of the amount of usage of IFS Services; and (iii) billing. Without limiting the generality of the foregoing, Client shall not retain or make copies of, and must purge from its system, the Queries and Answers prior to Client's receipt of any Score relating to such Queries and Answers; and in the event Client receives the IFS Services at its call center (or call center maintained by a Service Provider), Client shall ensure that the call center operators are unable to retrieve the Queries and Answers after the delivery of tie Score by, for example, disabling the use the back button key after the delivery of the Score- In the event that the IFS Services do not provide a response, tie Queries

must be purged as expeditiously as possible but in no event longer than thirty (30) minutes after receipt of such Queries.

Client has the right to transmit and authorize the use of ID Subject Content and hereby authorizes the use of ID Subject Content as required to perform the IFS Services; analyze, enhance or improve the performance of the IFS Services; and disclose ID Subject Content as required by law or the operation of the IFS Services. Client will timely, reliably and accurately relay the Queries, Answers and other 'D Subject Content to and from the IFS Services and the applicable ID Subject.

When providing ID Subjects with access to the IFS Services via the Internet, Client will adopt, publish, maintain and adhere to a privacy policy and upon request, provide a copy of Clients privacy policy.

Client's privacy policies clearly disclose to ID Subject that the ID Subject Content may be shared with third party service providers for the purpose of completing the relevant transaction.

Client acknowledges and agrees that prior to receiving the IFS Services, Client may need to complete an approval process for receipt of the IFS Services by the applicable wireless carriers. Such process shall include, without limitation, review of the proposed consumer consent language or any other consumer terms and conditions, review of any process flows, a description of Client's intended use, and a copy or summary of Client's applicable privacy policy. The IFS Service will be provided only with respect to those wireless carriers that have authorized the use of such data in connection with the provision of IFS Services, and then only to the extent and for the period that such data is available or provided by such wireless carriers.

Client will establish and maintain a manual verification process in the event that Client determines that an ID Subject does not pass the Risk Decision Threshold or Client receives a nag from tie IFS Services indicating a possible match from a fraud database.

Client will not (i) use or access the IFS Services outside the territorial boundaries of the United States, Canada, and the United States territories of Puerto Rico, Guam, and the Virgin Islands (collectively, the "Permitted Territory"); regardless of whether such use or access is by off-shore Authorized Agents or authorized Service Providers or an off-shore department or division of Client, or (it) export or permit the export of the IFS Services outside of the Permitted Territory. Client will not share or permit the use of the IFS Services, in whole or in part, with any third party.

Credit Bureau may review Client's practices and procedures including, without limitation, any relevant documentation, to determine Clients compliance with this Integrator Schedule- Client shall promptly provide Credit Bureau with copies of all requested documents and records- If Credit Bureau reasonably believes a compliance issue exists, Credit Bureau or its designated representative may enter Client's facilities, upon at least five (5) business days prior written notice and at a mutually agreed upon

time„ to an on-site assessment of Clients practices and procedures relating to Client's request for, and use of, the IFS Services and Client's security practices with respect thereto.

Client shall employ decision-making processes appropriate to the nature of the transaction and in accordance with industry standards, and Client will use the IFS Services only for the purposes set forth in this Integrator Schedule. Client is solely responsible for all results of its use of the IFS Services. TO THE MAXIMUM EXTENT ALLOWABLE BY LAW, ALL IFS SERVICES ARE PROVIDED BY Credit Bureau ON AN "AS-IS," AS-AVAILABLE BASIS, AND Credit Bureau (AND ITS DATA PROVIDERS AND SUPPLIERS HEREBY DISCLAIM ANY AND ALL PROMISES, REPRESENTATIONS, GUARANTEES, AND WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING WITH RESPECT TO THE ACCURACY, COMPLETENESS, CURRENTNESS, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, OF THE IFS SERVICES. IN NO EVENT WILL Credit Bureau OR ITS DATA PROVIDERS AND SUPPLIERS BE LIABLE TO CLIENT FOR ANY LOSS OR INJURY RELATING TO, ARISING OUT OF, OR CAUSED IN WHOLE OR IN PART BY, ITS ACTS OR OMISSIONS, EVEN IF NEGLIGENT, RELATING TO THE IFS SERVICES.

If Client receives the one-time passcode ("OTP"), Client must comply with the following acceptable use policy ("AUP"):

Scope. Client must comply with this Acceptable Use Policy ("AUP") with regard to its use of and access to the one-time passcode ("OTP"). By using the OTP Client acknowledges and agrees to comply with this AUP. This AUP shall only apply to the OTP and not to any IFS Services otherwise described in the Agreement. Further, Client agrees to cooperate with NCC, any third-party service provider involved in providing the OTP, and governmental authorities in investigations of any alleged or perceived violation of any law, rule, regulation or the AUP. Upon the request of any third-party service provider, NCC may modify this AUP at any time in which case it will promptly notify Client and provide Client a copy therewith.

Restrictions on Use. Client agrees that it will not use the OTP in or for any illegal, fraudulent, unauthorized or improper manner or purpose and will only be used in compliance with all applicable laws, rules and regulations, including all applicable state, federal and international internet, data, telecommunications, telemarketing, "spam," and import/export laws and regulations, including the U.S. Export Administration Regulations. Without limiting the foregoing, Client agrees not to permit the OTP to be used to transmit or disseminate any:

(i) Junk mail, spam, or unsolicited material to persons or entities that have not agreed to receive such material or to whom Client or its customer do not otherwise have a legal right to send such material;

(ii) Material that infringes or violates any third party's intellectual property rights, rights of publicity, privacy, or confidentiality, or the rights or legal obligations of any wireless service provider or any of its customers or subscribers;

(iii) Material or data that is illegal, or material or data, as determined by Equifax (in Equifax's sole discretion) that is harassing, coercive, defamatory, libelous, abusive, threatening, obscene, or otherwise objectionable, materials that are harmful to minors, or materials the transmission of which could diminish or harm the reputation of Equifax or any third party service provider involved in the provision of the OTP;

(iv) Material or data that is alcoholic beverage-related (e.g. beer, wine, or liquor), tobacco-related (e.g. cigarettes, cigars, pipes, chewing tobacco), guns or weapons-related (e.g. firearms, bullets) illegal drugs-related (e.g. marijuana, cocaine), pornographic-related (e.g. adult themes, sexual content), crime-related (e.g. organized crime, notorious characters), violence-related (e.g. violent games), death –related (e.g. funeral homes mortuaries), hate-related (e.g. racist organizations) ,gambling-related (e.g. casinos, lotteries), specifically mentions any wireless carrier or copies or parodies the products or services of any wireless carrier;

(v) Viruses, Trojan horses, worms, time bombs, cancel-bots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data, or personal information;

(vi) Material or information that is false or misleading;

(vii) Material that would expose any third party service provider involved in providing the OTP, or any other third party to liability; and/or

(viii) Any signal or impulse that could cause electrical, magnetic, optical, or other technical harm to the equipment or facilities of NCC or any third party.

Client shall not access any carrier services that Client has not ordered or for which Client has not paid applicable fees. Client will not use or attempt to use a third party's account with NCC or any third party service provider involved in providing the OTP, or interfere with the security of, or otherwise abuse, the OTP or any other third party service provider 's customers. Client shall not interfere in any manner with Equifax's provision of the OTP.

Client further acknowledges and agrees that all customers of Client and any third parties to whom messages may be transmitted using the OTP have the right to opt-in and opt-out of Short Message Services.

9. Requirements for Equifax Identity Scan Service

Equifax Identity Scan "Identity Scan" is an on-line warning system containing information that can be used to detect possible or known identity theft and application

fraud. Some of the information in the Identity Scan database is provided by credit grantors. If Client orders the Identity Scan service, then Client agrees to furnish for potential inclusion in Equifax's Identify Scan system any data that Client knows to have been used in connection with a fraudulent transaction or attempted fraudulent transaction with Client. That data will include but not be limited to consumer names, aliases, Social Security numbers, addresses (current and former), employment (current and former) and telephone numbers (business and residential). Client grants Equifax permission to evaluate and include such data in Identity Scan and other identity/ fraud products if deemed appropriate by Equifax and permits Equifax to use such information to test effectiveness of fraud and identity products. Subscriber will not use an alert or warning message from the Identity Scan system in its decision-making process for denying credit but will use the message as an indication that the consumer's application information should be independently verified prior to a credit decision. Client understands that the information supplied by Identity Scan may or may not apply to the consumer who has applied to Client for credit. Subscriber also understands and agrees that data from the Identity Scan system is proprietary to Equifax and shall not be used as a component of any database or file built or maintained by Client. The use of such data shall be limited to the specific transaction for which the Identity Scan alert message is provided.

10. Requirements for Equifax Synthetic ID Fraud Alert

A. These terms and conditions apply to Client's receipt of and use of the Synthetic Fraud Alerts, as described below, and Client acknowledges it will request and receive the Synthetic Fraud Alert, subject to the terms of the additional terms and conditions set forth below.

B. Synthetic ID Alerts provide flags and attributes that can help identify synthetic identity fraud through the use of aggregated and anonymous authorized user transactions from a separate anonymous database of potential synthetic identity fraud transactions that may have association with the subject consumer.

C. When Synthetic ID Alerts are delivered with a credit report, Synthetic ID Alerts includes authorized user output fields (Authorized User Velocity & ID Discrepancy flags plus other associated authorized/terminated user counts) and a Final assessment flag. Although Synthetic ID Alert are not consumer reports, this version of the Synthetic ID Alert may only be purchased at the same time that Client purchases a consumer report in connection with the extension of credit or account review.

D. Synthetic ID Alerts are for identity fraud risk alert purposes[1] only and are not to be used for determining an individual's eligibility for credit or any other FCRA permissible purpose or in any way for the purpose of taking "adverse action," in whole or in part, against a consumer, as defined in the ECOA and. Regulation B, or for suspending a consumer's account. As such Client will not use the Synthetic ID Alert in its decision-making process for denying credit but will use the Synthetic ID Alerts as an indication that the consumer's identity and personally identifiable information should be

independently verified to form a reasonable belief that Client knows the true identity of the consumer. Client certifies that it shall use the Synthetic ID Alerts exclusively within Client's own organization for the purpose of identity fraud prevention and for no other purpose. Client will not resell or otherwise redistribute the Synthetic ID Alerts.

E. Client understands that the information supplied by Synthetic ID Alerts may or may not apply to the consumer who has applied to Client for credit, service, dealings, or other financial transactions.

F. Client also understands and agrees that the information contained in the Synthetic ID Alerts is proprietary to Equifax and shall not be used as a component of any database or file build or maintained by Client. The use of each Synthetic ID Alert shall be limited to one time use in conjunction with the specific transaction for which the Synthetic ID Alert is requested and provided. Client's obligations with regard to the use of the Synthetic Fraud Alerts will survive any termination for as long as the Synthetic ID Alerts are in Client's custody or control. EQUIFAX MAY, BY WRITTEN NOTICE TO CLIENT, IMMEDIATELY TERMINATE OR SUSPEND THE PROVISION OF THE SYNTHETIC ID ALERT SERVICE IF EQUIFAX HAS A REASONABLE BELIEF THAT CLIENT HAS VIOLATED THE TERMS AND CONDITIONS APPLICABLE TO THE SYNTHETIC ID ALERTS.

G. Equifax, and its data suppliers (including government agencies) (a) makes no warranty, express, implied or statutory, and specifically disclaims all warranties with respect to the Limited Access Death Master File information incorporated into the Synthetic ID Alerts (the **"Death Master Flag"),** including but not limited to, implied warranties of merchantability and fitness for any particular use or that use of the Death Master Flag constitutes compliance with any law or regulation; (b) assume no liability for any direct, indirect or consequential damages flowing from any use of any part of the Death Master Flag, including infringement of third party intellectual property or privacy rights; and (c) assume no liability for any errors or omissions in the Death Master Flag. The Death Master Flag contains inaccuracies. As such, neither Equifax, NTIS, nor the Social Security Administration which provides the Death Master Flag to NTIS, guarantees the accuracy of the Death Master Flag. The LADFM does not contain death records for all deceased persons. Therefore, the absence of a particular person in the Death Master Flag is not proof that the individual is alive. Further, it is possible for the records of a person who is not deceased to be included erroneously in the Death Master Flag. Client acknowledges and agrees that the Death Master Flag does not guarantee the identity of or information regarding any individual and that Client has processes in place to independently verify the information provided in the Death Master Flag.

H. Specifically with regard to the Death Master Flag included with the Synthetic ID Alerts, Client

certifies that:

(i) Its access to the Death Master Flag is appropriate because Client (i) has a legitimate fraud prevention interest, a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; (ii) has systems facilities, and procedures in place to safeguard such information, and experience in maintaining the confidentiality, security, and appropriate use of such information, (iii) agrees to satisfy such similar requirements, and (iv) it will provide a renewal certification from time to time upon request from Equifax.

(ii) It will not share the Death Master Flag with any person or entity unless they first meet the requirements of this section. Client understands that any successful attempt by any person to gain unauthorized access to or use of the Death Master Flag that Equifax may immediately terminate Client's access to the Synthetic ID Alerts. In addition, any successful attempt by any person to gain unauthorized access may under certain circumstances may result in penalties as prescribed in 15 CFR § 1110.200 levied on Client and the person attempting such access.

Client will take appropriate action to ensure that all persons accessing the Death Master Flag through it are aware of their potential liability for misuse and/or penalties for attempting to gain unauthorized access. Any such access or attempted access is a breach, or attempted breach, of security, and Client must immediately report such events to Equifax.

I. Client will provide, at a minimum, the fields noted as "Required." ** If only last 4 digits of SSN are provided on input, the following flags cannot be returned: Shared SSN (Name), SSN Verified, Invalid SSN and Death Master Hit Flags.

Field Name	Required	Preferred
First Name	Yes	
Middle Name		X
Last Name	Yes	
Address Line 1	Yes	
Address Line 2		X
City	Yes	
State	Yes	
Zip code	Yes	
SSN** Last 4 digits	Yes	
SSN** 9 digits		X
Date of Birth		X
Phone Number		X
Email		X

Client, at its own expense, will prepare and deliver to Equifax at mutually agreed to intervals (but no less than every ninety (90) days) and in a mutually agreeable form and medium its most current identity fraud performance feedback data **("Feedback Data").** Feedback Data will be used to configure and enhance the performance of products and services related to potentially fraudulent activity. For purposes of this Addendum, "performance" means identity fraud outcome of decisions at time of origination or account management. Client will encrypt all Feedback Data as directed by Equifax and comply with such data security policies as Equifax may from time to time make known to Client in writing. Client hereby grants to Equifax a perpetual, irrevocable right and license to use, distribute, modify, create derivative works from, and copy the Feedback Data, combine the Feedback Data with other data, incorporate the Feedback Data into current and future databases, use the Feedback Data to develop and enhance products and services, and share the Feedback Data with third parties in conjunction with the evaluation of products and services. Feedback Data provided to Equifax hereunder shall only be subject to the license provided herein and shall not be deemed Client Data or Client Confidential Information. Client will notify Equifax upon learning that any Feedback Data supplied is inaccurate or incomplete. Client will provide Equifax with any corrections or additional Feedback Data necessary to make the Feedback Data supplied complete and accurate and will implement procedures to avoid re-reporting Feedback Data that is inaccurate.

11. Terms Applicable to OFAC Alert

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, Client 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. Client 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 Client 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.

Click here to view current Experian Access Security Requirements (ASR)

Organizational Security and Risk Management

NCC will document and at least annually update its policies and procedures, as well as, security and compliance controls, in the following major categories to ensure the security of the Credit Bureau Data:

a. Organizational / Corporate charts
b. Document Employees Security Awareness Training
c. Incident Responses Log
d. Incident Response Plan
e. Risk Management Program
f. Secure Configuration Management
g. Asset Management
h. Access Control
i. Encryption and Cryptography
j. Network and Communications
k. Vulnerability Management
l. Monitoring and Logging
m. Physical and Environmental Security Controls
n. Data Classification and Handling
o. Protection of Privacy Information
p. Business Continuity and Disaster Recovery
q. Employee Onboarding
r. Employee Background Check
s. Employee Security Awareness
t. Insider Threat Investigation

u. Where permitted by applicable law, NCC may require a drug test for illegal substances be performed by a third party for applicants directly working with sensitive Credit Bureau Data and or systems

v. Where permitted by applicable law, NCC may require a criminal history screening for applicants directly working with sensitive Bureau Data and or systems

w. Every Client will be Office of Foreign Assets Control Verification (OFAC) screened against the US Treasury Specially Designated Nationals and Blocked Persons list for compliance with all applicable US regulations/requirements. This list can be found at **http://sdnsearch.ofac.treas.gov/**