State of Oklahoma
Office of Management and Enterprise Services

ADDENDUM 1 TO STATE OF OKLAHOMA CONTRACT WITH CASTLE BRANCH INC. RESULTING FROM SOLICITATION NO. 0900000357

This Addendum 1 ("Addendum") is an Amendment to the Contract awarded to Castle Branch Inc. ("Vendor") in connection with Solicitation 0900000357 ("Solicitation") and is effective February 5, 2019.

Recitals

Whereas, the Client issued a Solicitation for proposals to provide products and services related to Background Screens and Verifications (BSVS) for pre-employment and volunteer background checks;

Whereas, the Vendor submitted a proposal which contained exceptions to the Solicitation terms and various other Contract Documents; and

Whereas, the Client and Vendor have negotiated the final terms under which Vendor will perform the Services under the Contract.

Now, therefore, in consideration of the foregoing and the mutual promises set forth herein, the receipt and sufficiency of which are hereby acknowledged the parties agree as follows:

1. **Addendum Purpose.**

   This Addendum memorializes the agreement of the parties with respect to negotiated terms of the Contract that is being awarded to Vendor as of even date with execution of this Addendum. The parties agree that Vendor has not yet begun performance of work contemplated by the Solicitation.

2. **Negotiated Documents of the Contract.**

   2.1. The parties have negotiated certain terms of the Contract as follows:

      i. revisions to certain additional documents provided by Vendor as contained in Attachment A this Addendum;

ii. certain negotiated exceptions and additional terms to the Solicitation as contained in Attachment B to this Addendum; and

iii. the hosting agreement as contained in Attachment C to this Addendum.

2.2. Accordingly, any reference to a Contract Document refers to such Contract Document as it may have been amended. If and to the extent any provision is in multiple documents and addresses the same or substantially the same subject matter but does not create an actual conflict, the more recent provision is deemed to supersede earlier versions.

State of Oklahoma

By: _____

Name: James L. Reese, II

Title: Chief Information Officer

Date: February 5, 2019

Castle Branch Inc.

By: _____

Name: Lauren Henderson

Title: CFO

Date: January 31, 2019

CastleBranch

The Power to Make Informed Decisions.

ATTACHMENT A-1 TO
ADDENDUM 1 TO
STATE OF OKLAHOMA CONTRACT WITH
CASTLE BRANCH INC.
RESULTING FROM SOLICITATION NO. 0900000357

The Employment Credit Report Agreement (the "Agreement") is hereby amended as set forth below and supersedes all prior documents submitted by Castle Branch Inc. or discussed by the parties.

EMPLOYMENT CREDIT REPORT AGREEMENT

1. Client is a(n) governmental entity (type of business) and has a need for consumer credit information in connection with the evaluation of individuals for employment, promotion, reassignment or retention as an employee ("Consumer Report for Employment Purposes").

2. Client shall request Consumer Reports for employment purposes pursuant to procedures prescribed by Vendor from time to time only when it is considering the individual inquired upon for employment, promotion, reassignment or retention as an employee, and for no other purpose.

3. Client certifies that it will not request a Consumer Report for Employment Purposes unless:

   a. A clear and conspicuous disclosure is first made in writing to the consumer by Client before the report is obtained, in a document that consists solely of the disclosure that a consumer report may be obtained for employment purposes;

   b. The consumer has authorized in writing the procurement of the report; and

   c. Information from the Consumer Report for Employment Purposes will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

4. Client further certifies that before taking adverse action in whole or in part based on the Consumer Report for Employment Purposes, it will provide the consumer with:

   a. A copy of the Consumer Report for Employment Purposes; and

   b. A copy of the consumer's rights, in the format approved by the Federal Trade Commission.

5. Client shall use the Consumer Report for Employment Purposes only for a one-time use, and shall hold the report in strict confidence, and not disclose it to any third parties that are not involved in the employment decision, except to the extent required by the Oklahoma Open Records Act.

6. Client will maintain copies of all written authorizations for a minimum of seven (7) years from the date of inquiry.

7. Upon providing prior written notice and the opportunity to cure within a ten (10) day period, and with just cause, such as violation of the terms of this Agreement or a legal requirement, or a material change in existing legal requirements that adversely affects this Agreement, either party may, upon its election, cancel the agreement immediately.

8. 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.

9. Client shall pay a fee for each inquiry for any of Credit Report, according to the then current published fee schedule.

10. Vendor shall use good faith in attempting to obtain information from sources deemed reliable, but does not guarantee the accuracy of the information reported.

11. It is further agreed that upon prior notice and the opportunity to cure within a ten (10) day period, and with just cause, such as delinquency or violation of the terms of the contract or a legal requirement, either party may, upon its election, cancel this Agreement immediately.

12. The parties hereto agree that this instrument is the full and complete Agreement between them regarding the furnishing of Credit Reports, and is not to be altered, varied, or enlarged upon by any verbal promises, statements, or representations not expressed herein. This Agreement shall not be binding on either party until accepted by Vendor.

ATTACHMENT A-2 TO
ADDENDUM 1 TO
STATE OF OKLAHOMA CONTRACT WITH
CASTLE BRANCH INC.
RESULTING FROM SOLICITATION NO. 0900000357

The Statement of Service-Equifax Verification Services ("SOS") is hereby amended as set forth below and supersedes all prior documents submitted by Castle Branch Inc. or discussed by the parties.

Statement of Service – Equifax Verification Services ("SOS")

BACKGROUND:

A. Client is party to a Contract with Vendor (the "**MSA**").

B. From time-to-time, Client procures from Vendor employment verification services ("**Verification Services**") pursuant to the SOS (the "**SOS - Verifications**").

C. Equifax Workforce Solutions, a/k/a Equifax Verification Services, a/k/a Equifax Verification Solutions (collectively, "**EVS**") operates a service for subscribing employers that provides employment verification information and data ("**EVS Employment Information**").

D. Certain employers require that all employment verification requests be made through EVS and, in such circumstances, Vendor is only able to obtain employment verification for applicants or employees of that employer through EVS.

E. Client desires that Vendor conduct employment verifications through EVS when required by the employer with which employment information is being verified.

F. Client agreed in the SOS - Verifications that Vendor may use EVS to provide Verification Services to Client, and Client agreed to pay any pass-through outsourcing fees charged in connection with the use of EVS.

G. EVS requires that Client agree to the provisions contained herein as a condition to Vendor's use of EVS for Client and provision of EVS Employment Information to Client.

AGREEMENT:

1. This SOS is incorporated into the MSA and the SOS - Verifications. To the extent this SOS may conflict with the terms of the MSA and any SOS - Verifications, the terms of this SOS shall control.

2. Client acknowledges and agrees that any failure of Client to agree to Vendor this SOS shall result in a cessation of Vendor's use of EVS to provide Verification Services to Client. In such event, the Verification Services provided to Client will not result in any information about an employee or applicant if the current or past employer of the employee or applicant uses EVS to respond to employment verification requests.

3. Client desires that Vendor use EVS to provide Verification Services as necessary for Client and to provide to Client EVS Employment Information.

4. Client agrees to pay to Vendor any pass-through outsourcing fees charged in connection with the use of EVS and the provision to Client of EVS Employment Information; provided, however, if Vendor agrees to charge the employee or applicant directly for Verification Services, then such amounts will be billed to the employee or applicant.

5. Any EVS Employment Information will be requested only for Client's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted by law, specifically including the Oklahoma Open

Records Act. Only designated representatives of Client will request EVS Employment Information on Client's employees, and employees will be forbidden to obtain EVS Employment Information on themselves, associates or any other persons except in the exercise of their official duties. Client will not disclose EVS Employment Information to the subject of the EVS Employment Information except as permitted or required by law, but will refer the subject to EVS or Vendor.

6. Client will hold EVS and all its agents harmless on account of any expense or damage arising or resulting from the publishing or other disclosure of EVS Employment Information by Client, its employees or agents contrary to the conditions of Section 5 above or applicable law.

7. Client recognizes that EVS does not guarantee the accuracy or completeness of EVS Employment Information.

8. Client (or, if agreed by Vendor, the applicant or employee) will be charged for the EVS Employment Information by Vendor, which is responsible for paying EVS for the EVS Employment Information; provided, however, should the underlying relationship between Client and Vendor terminate at any time during the term of this SOS, and Client procures directly from EVS the EVS Employment Information, charges for the EVS Employment Information will be invoiced to Client, and Client will be solely responsible to pay EVS directly.

9. Fair Credit Reporting Act Certification. Client certifies that it will order EVS Employment Information, which is a consumer report as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FCRA"), only when Client intends to use the EVS Employment Information: (a) in accordance with the FCRA and all state law counterparts; and for the following permissible purpose: for employment purposes; provided, however, that Client certifies that, before ordering EVS Employment Information to be used in connection with employment purposes, it will and did clearly and conspicuously disclose to the consumer, in a written document consisting solely of the disclosure, that Client may obtain EVS Employment Information for employment purposes, and it will and did also obtain the consumer's written authorization to obtain or procure EVS Employment Information relating to that consumer. Client further certifies that it will not take adverse action against the consumer based in whole or in part upon the EVS Employment Information without first providing to the consumer to whom the EVS Employment Information relates a copy of the EVS Employment Information and a written description of the consumer's rights as prescribed by the Consumer Financial Protection Bureau ("CFPB") under Section 609(c)(3) of the FCRA as referenced on Exhibit A-1 attached hereto, and also will not use any EVS Employment Information in violation of any applicable federal or state equal employment opportunity law or regulation. Client will use EVS Employment Information ordered under this SOS for the foregoing purpose and for no other purpose. Client acknowledges that it has received from Vendor a copy of the consumer rights summary as prescribed by the CFPB as referenced on Exhibit A-1.

It is recognized and understood that the FCRA provides that anyone "who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two (2) years, or both." EVS may, with reasonable advance notice, y conduct audits, not to exceed twice per year, of Client regarding its compliance with the FCRA and other certifications in this SOS. Audits will be conducted by email whenever possible and will require Clients to provide documentation as to permissible use of particular EVS Employment Information. In addition, Vendor will be required to provide documentation indicating Vendor validated the legitimacy of Client prior to contract execution and will also provide a copy of agreement between Vendor and Client. Client gives its consent to EVS to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Client's material breach of this Agreement, constitute grounds for immediate suspension of the service or termination of this SOS and Client's access to EVS and EVS Employment Information.

Vermont Certification. Client certifies that it will comply with applicable provisions under Vermont law when ordering EVS Employment Information relating to Vermont residents that are consumer reports as defined by the Vermont Fair Credit Reporting Act ("**VFCRA**"). In particular, Client certifies that it will order EVS Employment Information relating to Vermont residents that are consumer reports as defined by the VFCRA only after Client has received prior Consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Client further certifies that a copy of Section 2480e of the Vermont Fair Credit Reporting Statute, attached hereto as Exhibit A-2, was received from Vendor. Client will comply with the applicable provisions of the FCRA, Federal Equal Credit Opportunity Act and any amendments to it, all state law counterparts of them, and all applicable regulations promulgated under any of them including, without limitation, any provisions requiring adverse action notification to the Consumer.

10. Data Security. This Section 10 applies to any means through which Client orders or accesses EVS Employment

Information including, without limitation, system-to-system, personal computer or the Internet. The term "Authorized User" for purposes of this SOS means a Client employee of a consolidated agency that Client has authorized to order the EVS Employment Information and who is trained on Client's obligations under this SOS with respect to the ordering and use of the EVS Employment Information, including Client's FCRA and other obligations with respect to the access and use of consumer reports. With respect to handling the EVS Employment Information, Client agrees to:

a. ensure that only Authorized Users can order or have access to EVS Employment Information;

b. ensure that Authorized Users do not order EVS Employment Information for personal reasons or provide them to any third party except as permitted by this SOS;

c. inform Authorized Users that unauthorized access to consumer reports may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment;

d. ensure that all devices used by Client to order or access the EVS Employment Information are placed in a secure location and accessible only by Authorized Users and that such devices are secured when not in use through such means as screen locks, shutting power controls off, or other commercially reasonable security procedures;

e. take all necessary measures to prevent unauthorized ordering of EVS Employment Information by any persons other than Authorized Users for permissible purposes, including, without limitation, (i) limiting the knowledge of the Client security codes, member numbers, User IDs, and any passwords Client may use (collectively, "Security Information"), to those individuals with a need to know, (ii) changing Client's user passwords at least every ninety (90) days, or sooner if an Authorized User is no longer responsible for accessing the EVS Employment Information, or if Client suspects an unauthorized person has learned the password, and (iii) using all security features in the software and hardware Client uses to order EVS Employment Information;

f. in no event access the EVS Employment Information via any hand-held wireless communication device, including but not limited to, web enabled cell phones, interactive wireless pagers, personal digital assistants (PDAs), mobile data terminals, and portable data terminals;

g. not use non-company owned assets such as personal computer hard drives or portable and/or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs, and DVDs) to store EVS Employment Information;

h. encrypt EVS Employment Information when it is not in use and with respect to all printed EVS Employment Information store in a secure, locked container when not in use and completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose;

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

j. monitor compliance with the obligations of this Section 10, and immediately notify EVS if Client suspects or knows of any unauthorized access or attempt to access the EVS Employment Information, including, without limitation, a review of EVS invoices for the purpose of detecting any unauthorized activity;

k. not ship hardware or software between Client's locations or to third parties without deleting all Security Information and any EVS Employment Information;

l. use commercially reasonable efforts to assure data security when disposing of any consumer information or record obtained from the EVS Employment Information. Such efforts must include the use of those procedures issued by the federal regulatory agency charged with oversight of Client's activities (e.g. the Consumer Financial Protection Bureau, the applicable banking or credit union regulator) applicable to the disposal of consumer report information or records;

m. use commercially reasonable efforts to secure EVS Employment Information when stored on servers, subject to the following requirements: (i) servers storing EVS Employment Information must be separated from the internet or

other public networks by firewalls which are managed and configured to meet industry accepted best practices, (ii) protect EVS Employment Information through multiple layers of network security, including but not limited to, industry-recognized firewalls, routers, and intrusion detection/prevention devices (IDS/IPS), (iii) secure access (both physical and network) to systems storing EVS Employment Information, which must include authentication and passwords that are changed at least every ninety (90) days; and (iv) all servers must be kept current and patched on a timely basis with appropriate security specific system patches, as they are available;

n. not allow EVS Employment Information to be displayed via the internet unless utilizing, at a minimum, a three-tier architecture configured in accordance with industry best practices; and

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

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

11. Client certifies that it has read the attached Exhibit A-3 "Notice to Users of Consumer Reports, Obligations of Users" which explains Client's obligations under the FCRA as a user of consumer information.

Exhibit A-1 to CRA Qualified Subscriber Terms and Conditions
Summary of Consumer's Rights Under the Fair Credit Reporting Act

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. **For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.**

- **You must be told if information in your file has been used against you.** Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information.
- **You have the right to know what is in your file.** You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if:
  - a person has taken adverse action against you because of information in your credit report;
  - you are the victim of identify theft and place a fraud alert in your file;
  - your file contains inaccurate information as a result of fraud;
  - you are on public assistance;
  - you are unemployed but expect to apply for employment within 60 days.

  In addition, all consumers are entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.consumerfinance.gov/learnmore for additional information.
- **You have the right to ask for a credit score.** Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.
- **You have the right to dispute incomplete or inaccurate information.** If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. See www.consumerfinance.gov/learnmore for an explanation of dispute procedures.
- **Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.** Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.
- **Consumer reporting agencies may not report outdated negative information.** In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.
- **Access to your file is limited.** A consumer reporting agency may provide information about you only to people with a valid need – usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.
- **You must give your consent for reports to be provided to employers.** A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. For more information, go to www.consumerfinance.gov/learnmore.
- **You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.** Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).
- **You may seek damages from violators.** If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.
- **Identity theft victims and active duty military personnel have additional rights.** For more information, visit www.consumerfinance.gov/learnmore.

States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General. For information about your federal rights, contact:

TYPE OF BUSINESS:	CONTACT:
1.a. Banks, savings associations, and credit unions with total assets of over $10 billion and their affiliates. b. Such affiliates that are not banks, savings associations, or credit unions also should list, in addition to the CFPB:	a. Consumer Financial Protection Bureau 1700 G Street NW Washington, DC 20552 b. Federal Trade Commission: Consumer Response Center - FCRA Washington, DC 20580 (877) 382-4357
2. To the extent not included in item 1 above: a. National banks, federal savings associations, and federal branches and federal agencies of foreign banks b. State member banks, branches and agencies of foreign banks (other than federal branches, federal agencies, and Insured State Branches of Foreign Banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act c. Nonmember Insured Banks, Insured State Branches of Foreign Banks, and insured state savings associations d. Federal Credit Unions	 a. Office of the Comptroller of the Currency Customer Assistance Group 1301 McKinney Street, Suite 3450 Houston, TX 77010-9050 b. Federal Reserve Consumer Help Center P.O. Box 1200 Minneapolis, MN 55480 c. FDIC Consumer Response Center 1100 Walnut Street, Box #11 Kansas City, MO 64106 d. National Credit Union Administration Office of Consumer Protection (OCP) Division of Consumer Compliance and Outreach (DCCO) 1775 Duke Street Alexandria, VA 22314
3. Air carriers	Asst. General Counsel for Aviation Enforcement & Proceedings Aviation Consumer Protection Division Department of Transportation 1200 New Jersey Avenue, SE Washington, DC 20590
4. Creditors Subject to Surface Transportation Board	Office of Proceedings, Surface Transportation Board Department of Transportation 395 E Street, SW Washington, DC 20423
5. Creditors Subject to Packers and Stockyards Act, 1921	Nearest Packers and Stockyards Administration area supervisor
6. Small Business Investment Companies	Associate Deputy Administrator for Capital Access United States Small Business Administration 409 Third Street, SW, 8th Floor Washington, DC 20416
7. Brokers and Dealers	Securities and Exchange Commission 100 F Street, NE Washington, DC 20549
8. Federal Land Banks, Federal Land Bank Associations, Federal Intermediate Credit Banks, and Production Credit Associations	Farm Credit Administration 1501 Farm Credit Drive McLean, VA 22102-5090
9. Retailers, Finance Companies, and All Other Creditors Not Listed Above	FTC Regional Office for region in which the creditor operates *or* Federal Trade Commission: Consumer Response Center - FCRA Washington, DC 20580 (877) 382-4357

I.

Exhibit A-2 to CRA Qualified Subscriber Terms and Conditions
State Compliance Matters
Vermont Fair Credit Reporting Contract Certification

The undersigned, _____ ("Subscriber"), acknowledges that it subscribes to receive various information services from TALX Corporation, a provider of Equifax Verification Solutions ("EVS") in accordance with the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e (1999), as amended (the "VFCRA") and the Federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. Seq., as amended (the "FCRA") and its other state law counterparts. In connection with Subscriber's continued use of EVS information services in relation to Vermont consumers, Subscriber hereby certifies as follows:

Vermont Certification. Subscriber certifies that it will comply with applicable provisions under Vermont law. In particular, Subscriber certifies that it will order EVS Employment Information relating to Vermont residents, that are credit reports as defined by the VFCRA, only after Subscriber has received prior consumer consent in accordance with VFCRA § 2480e and applicable Vermont Rules. Subscriber further certifies that the attached copy of § 2480e of the Vermont Fair Credit Reporting Statute was received from EVS.

Subscriber:_____ (please print)

Signed By:_____

Printed Name:_____

Title:_____

Account Number:_____

Date:_____

Please also include the following information:

Compliance Officer or Person Responsible for Credit Reporting Compliance

Printed Name:_____

Title:_____

Mailing Address:_____

City:_____ State:_____ Zip:_____

E-Mail Address:_____

Phone:_____ Fax:_____

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

§ 2480e. Consumer consent

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

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

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

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

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

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

(2) the use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Consumer Financial Protection Bureau.

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

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

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

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

Exhibit A-3 TO CRA Qualified Subscriber Terms and Conditions

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

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

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

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

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

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

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

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

B. Users Must Provide Certifications

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

C. Users Must Notify Consumers When Adverse Actions Are Taken

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

1. Adverse Actions Based on Information Obtained From a CRA

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

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

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

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

3. Adverse Actions Based on Information Obtained From Affiliates

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

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

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

E. Users Have Obligations When Notified of an Address Discrepancy

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

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

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

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

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

A. Employment Other Than in the Trucking Industry

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

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

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

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

B. Employment in the Trucking Industry

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

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

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

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

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

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

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in 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. Sections 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 preestablished criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and 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. The statement must include the address and toll-free telephone number of the appropriate notification system.

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

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

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

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

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

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

The CFPB's website, *www.consumerfinance.gov/learnmore*, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:

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

ATTACHMENT A-3 TO
ADDENDUM 1 TO
STATE OF OKLAHOMA CONTRACT WITH
CASTLE BRANCH INC.
RESULTING FROM SOLICITATION NO. 0900000357

The FCRA Certifications are hereby amended as set forth below and supersedes all prior documents submitted by Castle Branch Inc. or discussed by the parties.

FCRA CERTIFICATIONS

a. Client acknowledges that some or all of the products or services being procured or accessed under the Contract may constitute "consumer reports," "consumer credit reports," or "investigative consumer reports" as such terms are defined in the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., and any regulations promulgated thereunder, as amended from time-to-time (collectively, the "**FCRA**") or applicable state or local laws (sometimes collectively referred to herein as "**consumer reports**"). Client shall not request or obtain, or permit its employees, agents, contractors, or representatives to request, access, or obtain, consumer reports or other information from Vendor for resale or transfer to, or use of, any other individual, entity, association, or organization unless specifically authorized by Vendor. All consumer reports and other information provided or otherwise made available by Vendor to Client or any other entity, organization, association, or individual in connection with the Contract, the products or services, or otherwise are current only as of the date provided on the report or information. All "medical information", as defined under the FCRA (including, without limitation, immunization records), and any other records, information, or documents uploaded, input, or transmitted to Vendor by Client or any individual in connection with the products or services provided or made available under the Contract, are provided, made available, and stored "AS IS," and Vendor makes no, and expressly disclaims all, representations and warranties, express or implied, regarding the completeness, accuracy, or validity of any such records, documents, or information. Client agrees that Vendor is not responsible or liable to Client or any other individual, entity, or organization for the record keeping practices of third parties, or errors or omissions in the records or information of third parties that is provided or made available to Client, including, but not limited to, the department of motor vehicles; county, state and federal courts; state repositories; state and regional prisons; local police stations; federal bankruptcy courts; federal civil courts; state medical boards; drug testing facilities or specimen collection sites; professional licensing organizations; and other local, state, and federal organizations and agencies.

b. Client acknowledges that Vendor is not a law firm, is not providing legal advice to Client, and does not guarantee or warrant Client's compliance with applicable laws regarding Client's procurement, use, storage, disclosure, protection, or destruction of information or consumer reports. Vendor may make available to Client sample forms or other documents which may include, but are not limited to, sample consumer report disclosure forms, sample consumer report authorizations, sample pre-adverse action notices, and sample adverse action notices (collectively, "**Sample Forms**"). Client acknowledges and agrees that any Sample Forms that are provided or made available by Vendor are only samples and do not constitute legal advice. Vendor shall have no liability or responsibility regarding Sample Forms. Vendor expressly disclaims any warranties, representations, or responsibility or damages associated with or arising out of Sample Forms or any information contained therein. Client understands and agrees that it is Client's responsibility to consult with its own legal counsel regarding Client's compliance with federal, state, and local laws, rules, and regulations, specifically including, without limitation, the FCRA and any laws, rules, or regulations relating to the procurement, use, storage, disclosure, protection, and destruction of information or consumer reports.

c. Client agrees to abide by all Ban the Box laws and other similar laws and regulations (including, without limitation, any prohibition or restriction on requesting or obtaining salary history information or criminal

history information) and certifies that, if required under applicable law, it will not conduct a background check until after a conditional offer of employment has been provided. Client accepts full and exclusive responsibility for complying with all such laws and for using the information and consumer reports it receives from Vendor in a legally acceptable fashion.

d. Client agrees to take precautionary measures to protect the security and confidentiality of all consumer report or other information including, for example, restricting terminal access, utilizing passwords to restrict access to terminal devices, and securing access to, dissemination, and destruction of electronic and hard copy reports. Client agrees that (i) only authorized employees of Client whose employment duties involve the procurement or use of consumer reports will procure, access, or use consumer reports from Vendor; and (ii) all consumer reports obtained by Client will be kept confidential in accordance with all applicable laws and that no information from any consumer report will be disclosed except as permitted by law, including, in particular, the Oklahoma Open Records Act.

e. Client represents, warrants, and certifies to Vendor that it is obtaining and using consumer reports from Vendor solely for the following permissible purposes under the FCRA, and for no other purpose: (i) employment purposes, or (ii) in accordance with the written instructions of the consumer.

f. With respect to each consumer report requested, obtained, accessed, or used by Client, Client agrees and certifies, and shall agree and certify as requested by Vendor, as follows: (i) no information from any consumer report will be used in violation of any applicable federal, state, or local equal employment opportunity law or regulation or other applicable law or regulation; (ii) Client made a clear and conspicuous disclosure in writing to the individual with respect to whom a consumer report is being procured, before Client procured or caused to be procured the consumer report or investigative consumer report, in a document that consists solely of the disclosure, that (1) a consumer report or investigative consumer report, if applicable (including information as to the consumer's character, general reputation, personal characteristics and mode of living, whichever are applicable), may be obtained by Client for employment purposes, (2) that, if applicable, the consumer report will include immunization records and other medical information to be used for employment purposes, specifically verifying the individual's compliance with Client or health care facility requirements for placement, accessing, teaching, or providing educational services at the facility, and (3) that the consumer has a right to, within a reasonable period of time after the receipt by the consumer of the disclosure, receive from Client a complete and accurate disclosure of the nature and scope of the investigation requested; (iii) the individual with respect to whom the consumer report or investigative consumer report is being procured authorized in writing the procurement of the consumer report or investigative consumer report by Client (including, if applicable, the procurement of immunization records or other medical information for use in employment purposes, specifically verifying the individual's compliance with Client or health care facility requirements for accessing, teaching, or providing educational services at the facility); and (iv) Client shall comply with all applicable laws, rules, and regulations relating to the procurement, use, storage, disclosure, privacy, confidentiality, security, or destruction of personally identifiable information or consumer reports, specifically including, without limitation, all applicable requirements of the FCRA. Client certifies and agrees that each time it orders or accesses a consumer report, it is reaffirming the above certifications.

g. Prior to taking adverse action based in whole or in part on information contained in a consumer report provided by Vendor, Client shall, and hereby certifies to Vendor that it shall, provide to the consumer: (1) a copy of the report, and (2) a description, in writing, of the rights of the consumer entitled: "A Summary of Your Rights Under the Fair Credit Reporting Act." After the appropriate waiting period, if the Client takes an adverse action based in whole or in part on such information, Client shall, and hereby certifies to Vendor that it shall, issue to the consumer a notice of the adverse action taken, including the statutorily required notices identified in Section 615 of the FCRA. Before taking adverse action based on a criminal record the EEOC Criminal History Guidance recommends performing an individualized assessment and/or other considerations and, if required by applicable law or regulation, Client agrees to perform an individualized assessment and/or other considerations before taking any adverse action based on a criminal record. To obtain a copy of the EEOC Criminal History Guidance please go to the following website: http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm.

h. Client agrees that Vendor may, but shall not be obligated to, request copies of any and all written disclosures provided by Client to any consumer(s) and written authorizations executed or provided by any consumer(s) with respect to the procurement by Client from Vendor of services regarding such consumer(s). As soon as reasonably practicable following such request, but in no event later than ten (10) business days, Client shall provide to Vendor copies of all requested disclosures and authorizations. Vendor reserves the right to prepare and send, in its sole and absolute discretion, notices under Section 613 of the FCRA to applicable consumers.

i. In addition to the disclosure requirements identified above, if the consumer makes a written request within a reasonable amount of time, Client shall provide: (i) information about whether an investigative consumer report has been requested; (ii) if an investigative consumer report has been requested, written disclosure of the nature and scope of the investigation requested; and (iii) Vendor's contact information, including complete address and toll-free telephone number. This information will be provided to the consumer no later than five (5) days after the request for such disclosure was received from the consumer or such report was first requested, whichever is the latter.

j. Client certifies and acknowledges that it has received and reviewed the following Federal Trade Commission notices and rules, which can be located at the following web addresses:

   i. Notice to Users of Consumer Reports: Obligations of Users under the FCRA
   https://www.castlebranch.com/documents/obligations-of-users.pdf

   ii. Summary of Your Rights Under the FCRA
   https://www.castlebranch.com/documents/summary-of-your-rights-under-the-FCRA.pdf

   iii. Remedying the Effects of Identity Theft
   https://www.castlebranch.com/documents/remedying-the-effects-of-identity-theft.pdf

   iv. Disposal of Consumer Report Information and Records
   https://www.castlebranch.com/documents/disposal-of-consumer-report-information-and-records.pdf

k. Regarding any consumer report, consumer credit report, or investigative consumer report obtained or accessed by Client about a resident of California, Client certifies to Vendor that, under the Investigative Consumer Reporting Agencies Act, California Civil Code Sections 1786 et seq. ("**ICRA**"), and the Consumer Credit Reporting Agencies Act, California Civil Code Sections 1785.1 et seq.) ("**CCRAA**"), Client will do the following:

   i. Request and use consumer reports, consumer credit reports, and investigative consumer reports (collectively referred to in this subsection (k) as "**investigative consumer reports**") solely for permissible purpose(s) identified under California Civil Code Sections 1785.11 and 1786.12.

   ii. When, at any time, any investigative consumer reports are sought for employment purposes other than suspicion of wrongdoing or misconduct by the consumer who is the subject of the investigation, provide a clear and conspicuous disclosure in writing to the consumer, which solely discloses: (1) that an investigative consumer report may be obtained; (2) the permissible purpose of the investigative consumer report; (3) that information on the consumer's character, general reputation, personal characteristics and mode of living may be disclosed; (4) the name, address, telephone number, and website of the Consumer Reporting Agency conducting the investigation; and (5) the nature and scope of the investigation requested, including a summary of the provisions of California Civil Code Section 1786.22.

   iii. When, at any time, investigative consumer reports are sought for employment purposes other than suspicion of wrongdoing or misconduct by the consumer who is the subject of the investigation, only request an investigative consumer report if the applicable consumer has authorized in writing the procurement of the investigative consumer report.

iv. Provide the consumer a means by which he/she may indicate on a written form, by means of a box to check, that the consumer wishes to receive a copy of any investigative consumer reports that are prepared. If the consumer wishes to receive a copy of the investigative consumer report, Client shall send (or contract with another entity to send) a copy of the investigative consumer report to the consumer within three business days of the date that the investigative consumer report is provided to Client.

v. Under all applicable circumstances, comply with California Civil Code Sections 1785.20 and 1786.40 if the taking of adverse action is a consideration, which shall include, but may not be limited to, advising the consumer against whom an adverse action has been taken that the adverse action was based in whole or in part upon information contained in the investigative consumer report, informing the consumer in writing of Vendor's name, address, and telephone number, and provide the consumer of a written notice of his/her rights under the ICRA and the CCRAA.

ATTACHMENT B TO
ADDENDUM 1 TO
STATE OF OKLAHOMA CONTRACT WITH
CASTLE BRANCH INC.
RESULTING FROM SOLICITATION NO. 0900000357

Negotiated Exceptions to the Solicitation

The Solicitation is hereby amended as set forth below and supersedes all prior Exceptions submitted by Castle Branch Inc. or discussed by the parties.

RFP Section	Exception
A. General Provisions, A.28. Confidentiality	**A. General Provisions, A.28.3 Confidentiality is hereby added:** A.28.3: Notwithstanding anything in this Contract to the contrary, Supplier may at all times disclose Confidential Information to the individual with respect to whom the information relates, if requested by such individual in writing.
A. General Provisions, A.45 Ownership Rights	**A. General Provisions, A.45.1 Ownership Rights** **Second sentence is hereby deleted in its entirety and replaced with the following:** Moreover, except with regard to any deliverable based on the Utilities, and except with regard to data owned by an individual, the State shall be deemed the sole and exclusive owner of all right, title, and interest therein, including but not limited to all source data, information and materials furnished to the state, together with all plans, system analysis, and design specifications and drawings, completed programs and documentation thereof, reports and listing, all data and test procedures and all other items pertaining to the work and services to be performed pursuant to this Contract including all copyright and proprietary rights relating thereto.

ATTACHMENT C TO
ADDENDUM 1 TO
STATE OF OKLAHOMA CONTRACT WITH
CASTLE BRANCH INC.
RESULTING FROM SOLICITATION NO. 0900000357

This Hosting Agreement ("Hosting Agreement") is a Contract Document in connection with the Contract issued as a result of Solicitation No. 0900000357 (the "Contract") and entered into between Castle Branch Inc. ("Vendor") and the State of Oklahoma by and through the Office of Management and Enterprise Services ("Client" or "Customer"), the terms of which are incorporated herein. This Hosting Agreement is applicable to any Customer Data stored or hosted by Vendor in connection with the Contract. Unless otherwise indicated herein, capitalized terms used in this Hosting Agreement without definition shall have the respective meanings specified in the Contract.

I. Definitions

a. "Customer Data" shall mean all data supplied by or on behalf of Customer in connection with the Contract, excluding any confidential information of Vendor.

b. "Data Breach" shall mean the unauthorized access by an unauthorized person that results in the access, use, disclosure or theft of Customer Data.

c. "Non-Public Data" shall mean Customer Data, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by Customer because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Customer as Non-Public Data, or that a reasonable person would deem confidential.

d. "Personal Data" shall mean Customer Data that contains 1) any combination of an individual's name, social security numbers, driver's license, state/federal identification number, account number, credit or debit card number and/or 2) contains electronic protected health information that is subject to the Health Insurance Portability and Accountability Act of 1996, as amended.

e. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the hosted environment used to perform the services.

II. Customer Data

a. Customer will be responsible for the accuracy and completeness of all Customer Data provided to Vendor by Customer. Customer shall retain exclusive ownership of all Customer Data. Non-Public Data and Personal Data shall be deemed to be Customer's confidential information. Vendor shall restrict access to Customer Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

b. Vendor shall promptly notify the Customer upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Customer Data or Customer's use of the hosted environment. Vendor shall notify the Customer by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Vendor shall not respond to subpoenas, service or process, FOIA requests, and other legal request related to Customer without first notifying the Customer and obtaining the Customer's prior approval, which shall not be unreasonably withheld, of Vendor's proposed responses. Vendor agrees to provide its completed responses to the Customer with adequate time for Customer review, revision and approval.

c. Vendor will use commercially reasonable efforts to prevent the loss of or damage to Customer Data in its possession and will maintain commercially reasonable back-up procedures and copies to facilitate the reconstruction of any Customer Data that may be lost or damaged by Vendor. Vendor will promptly notify Customer of any loss, damage to, or unauthorized access of Customer Data. Vendor will use commercially reasonable efforts to reconstruct any Customer Data that has been lost or damaged by Vendor as a result of its negligence or willful misconduct. If Customer Data is lost or damaged for reasons other than as a result of Vendor's negligence or willful misconduct, Vendor, at the Customer's expense, will, at the request of the Client, use commercially reasonable efforts to reconstruct any Customer Data lost or damaged.

III. Data Security

a. Vendor will use commercially reasonable efforts, consistent with industry standards, to provide security for the hosted environment and Customer Data and to protect against both unauthorized access to the hosting environment, and unauthorized communications between the hosting environment and the Customer's browser. Vendor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice

and not less stringent than the measures the Vendor applies to its own personal data and non-public data of similar kind.

b. All Personal Data and Non-public Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, Vendor is responsible for encryption of Personal Data.

c. Vendor represents and warrants to the Customer that the hosting equipment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Vendor will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Vendor will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Customer by Vendor, Vendor will promptly notify Customer of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Vendor has used to remediate the virus. Should the virus propagate to Customer's IT infrastructure, Vendor is responsible for costs incurred by Customer for Customer to remediate the virus.

d. Vendor shall provide its services to Customer and its users solely from data centers in the U.S. Storage of Customer Data at rest shall be located solely in data centers in the U.S. Vendor shall not allow its personnel or contractors to store Customer Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Vendor shall permit its personnel and contractors to access Customer Data remotely only as required to fulfill Vendor's obligations under the Contract.

e. Vendor shall allow the Customer to audit conformance to the Contract terms. The Customer may perform this audit or contract with a third party at its discretion and at Customer's expense.

f. Vendor shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. Vendor may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

IV. Security Assessment

a. The Client requires any entity or third-party vendor hosting Oklahoma Customer Data to submit to a State Certification and Accreditation Review process to assess initial security risk. Vendor submitted to the review and met the Client's minimum security standards at time the Contract was executed. Failure to maintain the

Client's minimum security standards during the term of the Contract, including renewals, constitutes a material breach.

b. To the extent Vendor requests a different sub-contractor than the third-party hosting Vendor already approved by the Client, the different sub-contractor is subject to the Client's approval. Vendor agrees not to migrate Client's data or otherwise utilize a different third-party hosting Vendor in connection with key business functions that are Vendor's obligations under the Contract until the Client approves the third-party hosting Vendor's State Certification and Accreditation Review, which approval shall not be unreasonably withheld or delayed. In the event the third-party hosting Vendor does not meet the Client's requirements under the State Certification and Accreditation Review, Vendor acknowledges and agrees it may not utilize such third-party Vendor in connection with key business functions that are Vendor's obligations under the Contract, until such third party meets such requirements.

V. **Security Incident Notification and Responsibilities**: Vendor shall inform Customer of any Security Incident or Data Breach

a. Vendor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Customer Data, Vendor will coordinate with Customer prior to making any such communication.

b. Vendor shall report a Security Incident to the Customer identified contact set forth herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation (i.e. HIPAA requires notice to be provided within 24 hours).

c. Vendor shall: (i) maintain processes and procedures to identify, respond to and analyze Security Incidents; (ii) make summary information regarding such procedures available to Customer at Customer's request, (iii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Vendor; and (iv) documents all Security Incidents and their outcomes.

VI. **Data Breach Notification and Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data or Non-Public Data within the possession or control of Vendor.

a. Vendor, unless stipulated otherwise, shall promptly notify the Customer identified contact within 2 hours or sooner, unless shorter time is required by applicable law,

if it confirms that there is, or reasonably believes that there has been a Data Breach. Vendor shall (1) cooperate with Customer as reasonably requested by Customer to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

b. Unless otherwise stipulated, if a Data Breach is a direct result of Vendor's breach of its obligation to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Vendor shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by state law; (3) credit monitoring services required by state or federal law; (4) a website or toll-free numbers and call center for affected individuals required by state law – (2), (3) and (4) not to exceed the agency per record per person cost calculated for data breaches in the United States on the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the Data Breach; and (5) complete all corrective actions as reasonably determined by Vendor based on root cause.

c. If a Data Breach is a direct result of Vendor's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Vendor shall indemnify and hold harmless the Customer against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

VII. Notice: Contact information for Customer for notifications pursuant this Hosting Agreement are consistent with the Contract with a copy sent to:

Chief Information Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

And

Chief Information Security Officer
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

And

OMES Information Services General Counsel
3115 N. Lincoln Blvd
Oklahoma City, OK 73105

<u>For immediate notice which does not constitute written notice:</u>

OMES Help Desk
405-521-2444
helpdesk@omes.ok.gov
Attn: Chief Information Security Officer

VIII. Vendor Representations and Warranties: Vendor represents and warrants the following

a. The product and services provided under this Hosting Agreement do not infringe a third party's patent or copyright or other intellectual property rights.

b. Vendor will protect Customer's Non-Public Data and Personal Data from unauthorized dissemination and use with the same degree of care that each such party uses to protect its own confidential information and, in any event, will use no less than a reasonable degree of care in protecting such confidential information.

c. The execution, delivery and performance of the Contract, the Hosting Agreement and any ancillary documents and the consummation of the transactions contemplated by the Contract or any ancillary documents by Vendor will not violate, conflict with, or result in a breach of any provision of, or constitute a default (or an event which, with notice or lapse of time or both, would constitute a default) under, or result in the termination of, any written contract or other instrument between Vendor and any third parties retained or utilized by Vendor to provide goods or services for the benefit of the Customer.

d. Vendor shall not knowingly upload, store, post, e-mail or otherwise transmit, distribute, publish or disseminate to or though the Hosting Environment any material that contains software viruses, malware or other surreptitious code designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or circumvent any "copy-protected" devices, or any other harmful or disruptive program.

IX. Indemnity

a. Vendor's Duty of Indemnification. Vendor agrees to indemnify and shall hold the State of Oklahoma and State, its officers, directors, employees, and agents harmless from all liabilities, claims, damages, losses, costs, expenses, demands, suits and actions of third parties (including without limitation reasonable attorneys' fees) (collectively "Damages") (other than Damages that are the fault of Customer) arising from or in connection with Vendor's breach of its express representations and warranties or other obligations in this Hosting Agreement and the Contract. If a third party claims that any portion of the products or services provided by Vendor under the terms of the Contract or this Hosting Agreement infringes that party's

patent or copyright, Vendor shall defend and indemnify the State of Oklahoma and Customer against the claim at Vendor's expense and pay all related costs, damages, and attorney's fees incurred by or assessed to, the State of Oklahoma and/or Customer. The State of Oklahoma and/or Customer shall promptly notify Vendor of any third party claims and to the extent authorized by the Attorney General of the State, allow Vendor to control the defense and any related settlement negotiations. If the Attorney General of the State of Oklahoma does not authorize sole control of the defense and settlement negotiations to Vendor, Vendor shall be granted authorization to equally participate in any proceeding related to this section but Vendor shall remain responsible to indemnify Customer and the State of Oklahoma for all associated costs, damages and fees incurred by or assessed to the State of Oklahoma and/or Customer. Should the software become, or in Vendor's opinion, be likely to become the subject of a claim or an injunction preventing its use as contemplated under this Hosting Agreement, Vendor may, at its option (i) procure for the State the right to continue using the software or (ii) replace or modify the software with a like or similar product so that it becomes non-infringing.

X. Termination and Suspension of Service:

a. In the event of a termination of the Contract, Vendor shall implement an orderly return of Customer Data in a mutually agreeable format at a time agreed to by the parties and the subsequent secure disposal of Customer Data.

b. During any period of service suspension, Vendor shall not take any action to intentionally erase any Customer Data.

c. In the event of termination of any services or agreement in entirety, Vendor shall not take any action to intentionally erase any Customer Data for a period of:

   i. 10 days after the effective date of termination, if the termination is in accordance with the contract period

   ii. 30 days after the effective date of termination, if the termination is for convenience

   iii. 60 days after the effective date of termination, if the termination is for cause

After such period, Vendor shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited or otherwise stipulated, delete all Customer Data in its systems or otherwise in its possession or under its control. Notwithstanding anything to the contrary in this Hosting Agreement, Vendor may retain copies of all records, reports, information, and other documentation collected, received, produced, or compiled in connection with the

Contract for legal, accounting, and regulatory purposes including, to respond to disputes of individuals to which the records relate, to provide file copies to the applicable individual, to respond to litigation, and to respond to court, regulatory agency, or other subpoenas or orders.

d. The Client shall be entitled to any post termination assistance generally made available with respect to the services.

e. Vendor shall securely dispose of all requested data in all of its forms, such as disk, CD/DVD, backup tape and paper, when requested by the Customer. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to Customer.