eSOPH Platform Addendum

V05112026

1. Overview and Product Description

NEOGOV's eSOPH (Electronic Statement of Personal History) platform is a web-based software-as-a-service application designed to assist government agencies and other authorized entities in managing pre-employment background investigations. The eSOPH platform enables Customer to: (i) receive and manage personal history statements and supporting documentation submitted by Applicants; (ii) coordinate and track background investigation workflows; (iii) share and verify applicant background information across participating agencies within the eSOPH network; and (iv) access optional integrated third-party services, including social media screening and consumer credit reporting services, as described in this Addendum.

"Applicant" means any individual who submits information through the eSOPH platform in connection with Customer's pre-employment background investigation process.

"Applicant Data" means any data transmitted by or about an Applicant to the eSOPH platform.

"Entry" has the meaning set forth in Section 2.5 of this Addendum.

"**Submitted Personal History Statement"** or **"Submitted PHS**" has the meaning set forth in Section 2.5 of this Addendum.

If Customer is purchasing eSOPH pursuant to an Order Form, the following terms are hereby incorporated into the Services Agreement ("**eSOPH Addendum**"). This eSOPH Addendum forms part of the Services Agreement, and in the case of any conflict or inconsistency between the terms and provisions of this eSOPH Addendum and any other provision of the Services Agreement, the terms of this eSOPH Addendum shall control.

2. Cross-Agency Applicant Data Verification

2.1 Purpose and Consent

To deliver faster, more reliable, and seamless hiring processes, eSOPH offers a cross-agency verification feature that benefits all participating agencies. When an Applicant submits information through eSOPH, the platform will cross-verify the Applicant's responses against previously submitted information from the same individual across other agencies participating in the NEOGOV eSOPH network. This streamlined verification is designed to enhance accuracy, reduce inconsistencies, and accelerate background investigations.

By using eSOPH, Customer agrees that Applicant information submitted in eSOPH **may be shared exclusively with other participating agencies within the NEOGOV eSOPH platform solely for the limited purpose of verifying prior applicant responses.** This cross-agency data verification is designed solely to enhance accuracy and efficiency in background investigations and candidate evaluations. NEOGOV facilitates this verification on Customer's behalf with strict limitations on how the shared data is used, ensuring it remains solely for verification purposes within the eSOPH network.

2.2 eSOPH Basic Applicant Data

Customer acknowledges and understands that a core feature of eSOPH is the ability for Customer to determine whether an Applicant has been previously entered into the eSOPH system by another participating agency. The information disclosed to other participating agencies (**"eSOPH Basic Applicant Data"**) is limited to: agency name, position applied for, entered date, and closed date, along with the point of contact for the agency that previously entered the Applicant. If Customer removes or purges background files from eSOPH, eSOPH Basic Applicant Data will remain in the system and continue to be visible to other participating agencies. Customer, by executing an Order Form incorporating this eSOPH Addendum, acknowledges this feature and that NEOGOV cannot disable it.

2.3 Customer's Sharing of Applicant Data

The eSOPH platform enables Customer to share Applicant Data with third parties. If Customer or its authorized users share Applicant Data outside of the eSOPH platform, Customer must: (i) possess a valid, signed authorization from each Applicant whose data is to be shared, legally adequate to authorize such disclosure; (ii) refrain from violating any applicable law, policy, term, or regulation in connection with such sharing; and (iii) maintain the Applicant Data in a secure and private manner consistent with applicable privacy laws and regulations.

2.4 Applicant Authorization

Customer is solely responsible for obtaining all necessary authorizations, disclosures, and consents from Applicants prior to any collection, processing, or sharing of Applicant Data through eSOPH, including but not limited to any authorizations required under applicable state and federal law.

2.5 Applicant Entries or Submitted PHI's

For each Applicant, an authorized user must create an entry into eSOPH using one of two methods: (i) by directly entering the Applicant's legal name and identifying information into eSOPH (an "Entry"); or (ii) by generating an access code within eSOPH that allows Applicants to self-enroll, with each Applicant who accesses eSOPH via such access code also constituting an "Entry." Any authorized user, including Applicants, must be capable of entering into legally binding agreements.

"Submitted Personal History Statement" or "Submitted PHS" means a Personal History Statement completed and submitted by an Applicant to Customer through the applicable Product.

Customer acknowledges that fees may be based on either Entries or Submitted PHSs, as specified in the applicable Order Form. The maximum number of Entries and/or Submitted PHSs permitted during each Subscription Period may be set forth in the applicable Order Form. If Customer requires additional Entries or Submitted PHSs during the Subscription Period, Customer must execute an amended Order Form prior to exceeding the then-current limit. NEOGOV reserves the right to enforce the applicable Entry and/or Submitted PHS limit within the eSOPH system upon receipt of a signed amended Order Form.

2.6 Post-Termination Data Retention

Notwithstanding the foregoing, NEOGOV may retain and store the following data during and after the term of this Addendum: Applicant name, telephone number, mailing address, email address, year of birth, date entered into eSOPH, background investigation close date, position applied for, executed legal agreements related to use of eSOPH (including electronic signature agreements, terms of use, and privacy policies), and anonymized Applicant Data dissociated from Personally Identifiable Information. NEOGOV may use such retained data solely to comply with applicable law, to maintain eSOPH Basic Applicant Data functionality for other participating agencies as described in Section 2.2, and for cross-agency verification purposes described in Section 2.1. NEOGOV will not use such retained data for any other purpose without Customer's prior written authorization.

3. CJIS Compliance

3.1 Customer Obligations

Customer acknowledges that the eSOPH platform is designed for use by law enforcement and government agencies and may be subject to the Federal Bureau of Investigation's Criminal Justice Information Services ("CJIS") Security Policy. Customer is solely responsible for determining whether its use of eSOPH is subject to CJIS requirements and for ensuring its own compliance with all applicable CJIS obligations. Customer shall not transmit Criminal Justice Information ("CJI") as defined under the FBI CJIS Security Policy via SMS/text messaging or any non-secure method through eSOPH. Customer represents and warrants that its authorized users with access to CJI will meet all applicable CJIS requirements, including executing required nondisclosure agreements and maintaining current CJIS Security Awareness Training certifications where applicable.

3.2 NEOGOV Obligations

To the extent applicable to the Services provided under this Agreement, NEOGOV agrees to comply with the requirements of the FBI Criminal Justice Information Services (CJIS) Security Policy in its handling of Criminal Justice Information. NEOGOV will implement appropriate technical, physical, and administrative safeguards to protect CJI in accordance with the CJIS Security Policy. NEOGOV shall ensure that all NEOGOV employees and contractors granted access to Customer Data complete a background check and meet the requirements set forth by CJIS policy for such access. All such NEOGOV personnel shall execute nondisclosure agreements and a CJIS Security Addendum, and shall maintain a current CJIS Security Awareness Training certificate. Customer Data will be stored on servers located within the United States in accordance with the FBI CJIS Security Policy.

4. Customer Compliance Responsibility

4.1 Sample Forms. The eSOPH platform may include default or sample forms, fields, and templates for collecting information from Applicants (**"Sample Forms"**). Sample Forms are provided by NEOGOV on an "AS IS" basis with no warranty of any kind, express or implied. Customer is solely responsible for evaluating the suitability of any Sample Forms for Customer's particular use case and for ensuring compliance with all applicable laws and regulations. Customer understands that NEOGOV does not maintain or provide updates to Sample Forms or other content within the control of Customer through the eSOPH user interface. Customer is responsible for all updates to forms and content required to maintain compliance with its own internal policies and applicable laws.

4.2 Restrictions on Data Entry. Except as expressly permitted herein, Customer and its authorized users are strictly prohibited from entering fictitious data — including fictitious names, Social Security numbers, addresses, phone numbers, or other identifying information — into eSOPH at any time for testing, training, or any other purpose. Upon Customer's request, NEOGOV will provide a designated test applicant name and associated information sufficient for training and testing purposes. NEOGOV will remove the test applicant from eSOPH upon Customer's request following the completion of testing or training. Violation of this restriction may result in immediate suspension of Customer's access to eSOPH.

5. Social Media Screening Services (Optional)

This Section 5 applies only if Customer has subscribed to the Social Media Screening Service as listed in the applicable Order Form.

5.1 Service Description

As an optional add-on service, NEOGOV provides access to a third-party social media screening service integrated with the eSOPH platform (the **"Social Media Screening Service"**). Social media screening reports (**"Social Media Screening Reports"**) are generated by a third-party screening provider. The current provider is FAMA Technologies, Inc. ("**FAMA**"), though NEOGOV reserves the right to change providers as necessary to maintain appropriate service levels. The contents of Social Media Screening Reports constitute Applicant Data when entered into or stored in the eSOPH platform. Customer is solely responsible for ensuring the secure storage, delivery, and transmission of Social Media Screening Reports to and among its authorized users.

5.2 NEOGOV Disclaimer for Social Media Screening Service

NEOGOV MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, AS TO THE VALUE, ACCURACY, COMPLETENESS, TIMELINESS, OR SUITABILITY OF ANY SOCIAL MEDIA SCREENING REPORT OR THE SOCIAL MEDIA SCREENING SERVICE. NEOGOV ACTS SOLELY AS AN INTERMEDIARY BETWEEN CUSTOMER AND THE THIRD-PARTY SOCIAL MEDIA SCREENING PROVIDER (CURRENTLY FAMA). NEOGOV IS NOT THE PREPARER OF ANY SOCIAL MEDIA SCREENING REPORT AND SHALL HAVE NO LIABILITY FOR ANY CLAIM, LOSS, OR DAMAGE ARISING FROM THE CONTENT, ACCURACY, OR USE OF ANY SOCIAL MEDIA SCREENING REPORT. CUSTOMER USES THE SOCIAL MEDIA SCREENING SERVICE ENTIRELY AT ITS OWN RISK.

5.3 FCRA Compliance — Social Media Screening

Customer acknowledges that Social Media Screening Reports may constitute "consumer reports" under the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("**FCRA**"). Customer, and not NEOGOV, is solely responsible for compliance with the FCRA and all applicable state laws in connection with the use of Social Media Screening Reports. Without limiting the foregoing, Customer agrees to the following:

- **Permissible Purpose.** Customer certifies it will use Social Media Screening Reports solely for "employment purposes" as defined under 15 U.S.C. § 1681a, and for no other purpose.
- **Disclosure and Authorization.** Prior to procuring any Social Media Screening Report, Customer will: (i) provide a clear and conspicuous written disclosure to the Applicant, in a document consisting solely of the disclosure, that a Social Media Screening Report may be obtained; and (ii) obtain the Applicant's written authorization for procurement of the report.
- **Adverse Action Procedures.** Before taking any adverse action based in whole or in part on a Social Media Screening Report, Customer will provide the Applicant: (i) a copy of the report; (ii) a written description of the Applicant's consumer rights under the FCRA; and (iii) a statement that information from the report will not be used in violation of any applicable federal or state equal employment opportunity law.
- **EEO Compliance.** Customer will not use Social Media Screening Reports in violation of any applicable federal or state equal employment opportunity law or regulation.
- **Record Retention.** Customer is solely responsible for retaining all executed Applicant authorization agreements. Customer will provide NEOGOV with copies of such agreements within five (5) calendar days of NEOGOV's written request.

5.4 Permitted Use Restrictions — Social Media Screening

Customer shall not:

- Modify, copy, reverse engineer, or create derivative works from the Social Media Screening Service or its underlying software;
- Use the Social Media Screening Service for any purpose other than Customer's internal pre-employment screening;
- Distribute, resell, sublicense, or transfer access to the Social Media Screening Service to any third party;
- Use Social Media Screening Reports to build competitive products or services;
- Use the Social Media Screening Service to send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children, or in violation of any third-party privacy rights; or
- Gain unauthorized access to, or disrupt the integrity or performance of, the Social Media Screening Service.

5.5 Intellectual Property — Social Media Screening

Customer acknowledges that the Social Media Screening Service provider has expended substantial time, effort, and resources to create and deliver the Social Media Screening Service. All intellectual property rights in the Social Media Screening Service not related to the eSOPH platform belong exclusively to the Social Media Screening Service provider. Nothing in this Section 5 conveys to Customer any ownership interest in the intellectual property of the Social Media Screening Service provider.

5.6 Security Breach — Social Media Screening

In addition to any other data breach provisions in the Services Agreement, if Customer discovers that physical or electronic safeguards have been breached, or that unauthorized access to Applicant Data has occurred in connection with the Social Media Screening Service, Customer shall notify NEOGOV in writing within twenty-four (24) hours of discovery, including all information known as of the time of notification.

5.7 Termination — Social Media Screening

NEOGOV may terminate the Social Media Screening Service at any time, with or without cause or notice, in NEOGOV's sole discretion and without penalty. Termination of the Social Media Screening Service does not constitute termination of the eSOPH subscription or the Services Agreement.

6. Experian Credit Reporting Services (Optional)

This Section 6 applies only if Customer has subscribed to the Experian Services as listed in the applicable Order Form.

6.1 Service Description

As an optional add-on service, NEOGOV provides Customer with access, through the eSOPH platform, to consumer credit reports and related services made available by Experian Information Solutions, Inc. (**"Experian"**), including Employment Insight and Fraud Shield reports (collectively, **"Experian Services"** and each report generated thereunder, a **"Credit Report"**). Customer's use of the Experian Services is subject to the terms of this Section 6, the FCRA, and the then-current terms of Experian's subscriber agreement and applicable regulatory flow-down requirements, including but not limited to the FCRA Letter Agreement between Experian and Customer (the **"Experian Flow-Down Terms"**), which are hereby incorporated into this Addendum by reference to the extent applicable.

6.2 NEOGOV Disclaimer for Experian Services

NEOGOV MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, AS TO THE VALUE, ACCURACY, COMPLETENESS, TIMELINESS, OR SUITABILITY OF ANY EXPERIAN SERVICES, CREDIT REPORT, OR OTHER DATA PROVIDED BY EXPERIAN. NEOGOV ACTS AS AN INTERMEDIARY IN FACILITATING CUSTOMER'S ACCESS TO EXPERIAN SERVICES AND IS NOT RESPONSIBLE FOR THE CONTENT, ACCURACY, OR AVAILABILITY OF ANY CREDIT REPORT OR EXPERIAN DATA. NEOGOV SHALL HAVE NO LIABILITY FOR ANY CLAIM, LOSS, OR DAMAGE ARISING FROM THE CONTENT OR USE OF ANY CREDIT REPORT OR THE EXPERIAN SERVICES. CUSTOMER USES THE EXPERIAN SERVICES ENTIRELY AT ITS OWN RISK.

6.3 FCRA Compliance — Experian Services

Customer acknowledges that Credit Reports are "consumer reports" under the FCRA. Customer, and not NEOGOV, is solely responsible for FCRA compliance in connection with all use of the Experian Services. Customer agrees to comply with Experian's then-current "FCRA Requirements" notice and "Access Security Requirements," as may be updated by Experian from time to time upon notice to Customer, and to take all reasonable measures to enforce said requirements. Without limiting the foregoing, Customer agrees and certifies as follows:

- **Permissible Purpose.** Customer will request and use the Experian Services strictly in accordance with the FCRA and solely for "employment purposes" as defined under 15 U.S.C. § 1681, or another permissible purpose under the FCRA. Customer will not use Experian Services for purposes prohibited by law.
- **Disclosure and Authorization.** Prior to procuring any Credit Report for employment purposes, Customer will: (i) provide a clear and conspicuous written disclosure to the Applicant, in a standalone document, that a Credit Report may be obtained for employment purposes; and (ii) obtain the Applicant's written authorization for procurement of the report.
- **Summary of Consumer Rights.** Customer acknowledges receipt of the Summary of Consumer Rights prescribed by the Consumer Financial Protection Bureau under FCRA Section 609(c)(1) and agrees to attach a copy to each Credit Report used for employment purposes, as required by FCRA Section 604(b)(3)(A)(ii).
- **Adverse Action Procedures.** Before taking any adverse action based in whole or in part on a Credit Report, Customer will provide the Applicant: (i) a copy of the report; (ii) a written description of the Applicant's FCRA rights; and (iii) a statement that information from the Credit Report will not be used in violation of any applicable federal or state equal employment opportunity law.

- **Applicant Access to Report.** If an Applicant makes a timely request and applicable law requires Customer to share the contents of the Applicant's Credit Report, Customer will do so without charge and only after authenticating the Applicant's identity.
- **EEO Compliance.** Customer will not use Credit Reports in violation of any applicable equal employment opportunity law or regulation.
- **Record Retention.** Customer is solely responsible for retaining all executed Applicant authorization agreements and will provide NEOGOV with copies within five (5) calendar days of NEOGOV's written request.

6.4 Death Master File Certification

Customer acknowledges that Experian Services may contain information derived from the Death Master File ("DMF") as issued by the Social Security Administration. Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, Customer certifies that its use of any deceased flags or other DMF indicia within the Experian Services is restricted to legitimate fraud prevention or business purposes in compliance with applicable laws, rules, and regulations, or fiduciary duty, consistent with 15 C.F.R. § 1110.102(a)(1). Customer further certifies that it will not take any adverse action against any Applicant solely on the basis of DMF indicia without further investigation to verify such information.

6.5 Employment Insight Certifications

Where Customer uses the Employment Insight report product within the Experian Services, Customer certifies that: (a) prior to procuring an Employment Insight Report, a clear and conspicuous written disclosure has been made to the Applicant in a standalone document that an employment consumer report may be obtained; (b) the Applicant has authorized in writing the procurement of the report; (c) prior to taking any adverse action based in whole or in part on an Employment Insight Report, Customer will provide the Applicant with a copy of the report and a written description of the Applicant's FCRA rights; and (d) information from the Employment Insight Report will not be used in violation of any applicable federal or state equal employment opportunity law or regulation.

6.6 Fraud Shield Certifications

Where Customer uses the Fraud Shield product within the Experian Services, Customer: (a) agrees to use such services solely to validate a consumer's identity and not to establish an individual's eligibility for personal credit, insurance, or employment; and (b) certifies that it will not take any adverse action as defined under the FCRA against any consumer or deny access to Customer's services based in whole or in part on information obtained from Fraud Shield. In lieu of any adverse action based on Fraud Shield results, Customer should take additional steps to verify the Applicant's identity.

6.7 Written Instructions and Consumer Consent

Where Customer accesses consumer credit information online in connection with the Experian Services, Customer will prominently display a notice to each Applicant in substantially the following form, and the Applicant's affirmative consent must be obtained before proceeding:

> *"You understand that by clicking the 'I AGREE' button immediately following this notice, you are providing 'written instructions' to [Customer] under the Fair Credit Reporting Act authorizing [Customer] to obtain information from your personal credit profile or other information from Experian. You authorize [Customer] to obtain such information solely to [insert purpose]."*

Customer shall retain a record of each Applicant's written instruction in a form capable of being accurately reproduced for later reference. Where consent is obtained by telephone, Customer shall comply with equivalent telephonic consent procedures that satisfy the FCRA's written authorization requirements.

6.8 Data Security — Experian Services

Customer and NEOGOV each agree to, at minimum, meet the requirements of 16 C.F.R. § 314.4 and take all steps reasonably designed to: (i) ensure the security and confidentiality of the Experian Services and Applicant Data used

in connection therewith; (ii) protect against anticipated threats or hazards to the security or integrity of such data; and (iii) protect against unauthorized access that could result in substantial harm or inconvenience to any Applicant. Customer shall be solely responsible for the secure storage, delivery, and transmission of Experian Services and Credit Reports to and among its authorized users.

6.9 Use Restrictions — Experian Services

Customer shall not:

- Use Experian Services to build or compile a credit reporting database;
- Modify, copy, reverse engineer, or create derivative works from any Experian Service or Credit Report;
- Distribute, resell, sublicense, or transfer access to the Experian Services to any third party;
- Use Experian Services for any purpose other than Customer's internal pre-employment screening;
- Use the Experian Services to send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children, or in violation of any third-party privacy rights; or
- Gain unauthorized access to, or disrupt the performance or integrity of, the Experian Services.

6.10 Security Breach — Experian Services

In addition to any other data breach provisions in the Services Agreement, if Customer discovers that physical or electronic safeguards have been breached, or that unauthorized access to Applicant Data has occurred in connection with the Experian Services, Customer shall notify NEOGOV in writing within twenty-four (24) hours of discovery, including all information then known by Customer.

6.11 Point of Sale Certification

In compliance with Section 1785.14(a) of the California Civil Code, to the extent applicable, Customer certifies to Experian whether Customer is or is not a retail seller as defined in Section 1802.3 of the California Civil Code. Customer represents and warrants that its certification is accurate and that Customer will promptly notify NEOGOV of any change in its status that would affect such certification.

6.12 Intellectual Property — Experian Services

Customer acknowledges that Experian has expended substantial time, effort, and resources to create and deliver the Credit Reports and compile its databases. All data in Experian's databases and all other intellectual property related to the Experian Services belong exclusively to Experian. Nothing in this Section 6 conveys to Customer any ownership interest in Experian's intellectual property or data.

6.13 Termination — Experian Services

NEOGOV may terminate Customer's access to the Experian Services at any time, with or without cause or notice, in NEOGOV's sole discretion and without penalty. Termination of Experian Services does not constitute termination of the eSOPH subscription or the Services Agreement. In addition, Experian may require Customer to execute updated certifications or compliance documents, or may direct NEOGOV to suspend Customer's access to Experian Services if Customer fails to comply with FCRA or other applicable requirements.

7. Two-Way Text Messaging Feature (Optional)

The eSOPH platform includes an optional two-way text messaging feature that allows Customer and its authorized users to communicate with Applicants via SMS/text message (the **"Text Messaging Feature"**). The following terms apply if Customer activates or uses the Text Messaging Feature:

7.1 Customer Compliance. Customer is solely responsible for complying with all applicable laws governing text messaging, including without limitation the Telephone Consumer Protection Act (47 U.S.C. § 227) ("TCPA") and

all applicable state equivalents. Prior to sending any text message to an Applicant, Customer shall obtain all legally required prior express written consent from the Applicant.

7.2 Prohibited Content. Customer shall not transmit via the Text Messaging Feature: (i) Criminal Justice Information ("CJI") as defined under the FBI CJIS Security Policy; (ii) Social Security numbers or other government-issued identification numbers; or (iii) any information whose transmission via SMS/text is prohibited by applicable law.

7.3 Opt-Out and Consent Records. Customer shall maintain records of all Applicant consents obtained for text messaging and shall promptly honor any opt-out or revocation request. Customer shall provide NEOGOV with copies of consent records within five (5) calendar days of NEOGOV's written request.

7.4 Platform Role. NEOGOV provides the Text Messaging Feature solely as a platform conduit. Customer is the sender of all text messages transmitted through the feature. NEOGOV shall not be liable for the content of any text message sent by Customer or its authorized users.

8. General Disclaimer for Third-Party Integrated Services

THE SOCIAL MEDIA SCREENING SERVICE, EXPERIAN SERVICES AND TEXT MESSAGING SERVICES ARE THIRD-PARTY SERVICES THAT ARE MADE AVAILABLE THROUGH THE eSOPH PLATFORM FOR CUSTOMER'S CONVENIENCE. NEOGOV IS NOT THE PROVIDER, PREPARER, OR GUARANTOR OF ANY REPORTS, DATA, OR CONTENT GENERATED BY FAMA, EXPERIAN, OR ANY OTHER THIRD-PARTY PROVIDER. NEOGOV DOES NOT ENDORSE ANY THIRD-PARTY PROVIDER OR ITS SERVICES. NEOGOV'S AGGREGATE LIABILITY FOR CLAIMS ARISING FROM CUSTOMER'S USE OF ANY THIRD-PARTY INTEGRATED SERVICES SHALL BE GOVERNED BY THE LIMITATIONS OF LIABILITY SET FORTH IN THE SERVICES AGREEMENT. CUSTOMER ASSUMES ALL RESPONSIBILITY FOR COMPLIANCE WITH APPLICABLE LAWS, INCLUDING THE FCRA, IN CONNECTION WITH THE PROCUREMENT AND USE OF ANY THIRD-PARTY REPORTS OR DATA.

9. Data Privacy and Credit Reporting Disclaimer

NEOGOV does not act as a credit reporting agency, credit bureau, or provider of credit-related evaluations and makes no representations or warranties, express or implied, regarding the accuracy, completeness, or reliability of any information accessed or obtained through the eSOPH platform for credit-related purposes. Customer is solely responsible for compliance with all applicable laws and regulations governing credit reporting, employment screening, and financial decision-making, including without limitation the FCRA, applicable state equivalent statutes, and all applicable equal employment opportunity laws.

10. Conflict; Integration

This eSOPH Addendum is incorporated into and made a part of the Services Agreement. In the event of a conflict between this eSOPH Addendum and the body of the Services Agreement, this eSOPH Addendum shall control as to the subject matter hereof. Capitalized terms used but not defined in this eSOPH Addendum have the meanings ascribed to them in the Services Agreement.