SERVICE AGREEMENT

This Service Agreement ("Agreement"), effective as of the date of Sterling's signature ("Effective Date"), is made by and between Sterling Infosystems, Inc. d/b/a Sterling with offices located at 1 State Street Plaza, 24th Floor, New York, NY 10004 ("**Sterling**") and with offices located at ("**Client**"). In consideration of the mutual obligations set forth in this Agreement, each party agrees to the terms and conditions below and represents that this Agreement is executed by its duly authorized representative.

1. Services

1.1 Sterling shall make available to Client the services listed on Attachment 1, attached hereto, ("**Services**") through the applicable Sterling service platform listed on Attachment 1 ("**Platform**"). Sterling and Client agree that Client's orders for Services are expected to commence on or about (the "**Commencement Date**"). Any twelve (12) month period starting on the Commencement Date or anniversary thereof is referred to as a "**Contract Year**".

1.2 The initial term of this Agreement shall commence on the Commencement Date and continue for a term of thirty-six (36) months ("**Initial Term**"). Thereafter this Agreement shall automatically renew for successive terms equal in length to the Initial Term (each a "**Renewal Term**") unless either party gives notice of its intent not to renew at least seventy five (75) days prior to the end of the then current term. The Initial Term and any Renewal Terms constitute the "**Term**" of this Agreement. Sterling will not provide Services to Client until (i) Client has executed the Background Screening Requirements Addendum (the terms of which are incorporated by reference herein) and (ii) Sterling has approved Client's Credentialing Application. Client's affiliates and subsidiaries may use Sterling's Services under this Agreement, provided that (a) each such affiliate and subsidiary executes a separate Background Screening Requirement Addendum and Credentialing Application, as may be required by Sterling; and (b) Client is responsible for such affiliates' and subsidiaries' acts, omissions and compliance with this Agreement.

1.3 During the Term Sterling shall be Client's exclusive provider of employee screening services, including without limitation verifications, drug testing, criminal background searches, corporate due diligence.

2. Invoicing and Payment

2.1 Sterling will invoice Client monthly at the prices set forth on Attachment 1 and payment shall be due within thirty (30) days of the date of invoice. A late payment charge of the lesser of 1 ½% per month or the highest lawful rate may be applied to any outstanding balances until paid. Client shall also reimburse Sterling for all costs incurred in collecting any late payments, including, without limitation, reasonable attorneys' fees.

2.2 After the initial Contract Year, Sterling may revise pricing for Services upon thirty (30) days written notice. Client agrees that the pricing on Attachment 1 is based on Client's projected annual volume as set forth on Attachment 1. If Client's actual volume, by one or more measure on Attachment 1, as of the end of a Contract Year is less than 90% of such projected volume, Sterling may revise its pricing upon written notice to Client.

2.3 Pricing is exclusive of, and Client will pay, any taxes relating to this Agreement applicable to Client.

3. Restrictions on Use

3.1 Client will obtain and use any background check report, including any consumer report or investigative consumer report, as those terms are defined in the Fair Credit Reporting Act, as amended ("**FCRA**") (collectively "**Screening Reports**"), solely for the permissible purpose(s) designated by the Client in the Credentialing Application and in accordance with the requirements in the Background Screening Requirements Addendum. Client is responsible for ensuring that its use of the Services and Screening Reports complies with all applicable local, state, federal and international laws, rules, regulations or requirements, including, but not limited to the FCRA.

3.2 Client will not provide any part of the Services or Screening Reports to others, whether directly or indirectly, through incorporation in a database, report or otherwise.

4. Confidentiality

4.1 Client shall not disclose any Screening Reports, or any portion thereof, provided to it by Sterling hereunder except as permitted by this Agreement, required by law, or to the subject of the report.

4.2 Each party ("**Recipient**") will treat, and take all reasonable and necessary steps to prevent the disclosure of, all information provided by the other party ("**Discloser**") that Discloser designates in writing to be confidential (or that would be understood to be confidential by a reasonable person) in the same manner as Recipient treats its own confidential information (which shall be no less than a reasonable degree of care). Discloser represents and warrants that it has all necessary legal rights, title, consents and authority to disclose such confidential information to Recipient. Confidential information shall not include information that (i) is or becomes a part of the public domain through no act or omission of Recipient; (ii) was in Recipient's lawful possession prior to Discloser's disclosure to Recipient; (iii) is lawfully disclosed to Recipient by a third-party with the right to disclose such information and without restriction on such disclosure; or (iv) is independently developed by Recipient without use of or reference to the confidential information. Client shall not disclose the negotiated pricing or terms of this Agreement to any third party, except as required by applicable law.

5. Platform

5.1 Sterling will make the Platform available for access and use by Client through a modern web-browser. The Platform and Services may be provided to Client by Sterling and/or Sterling's subsidiary and affiliate companies ("Sterling Affiliates").

5.2 Sterling will maintain reasonable safeguards for the Platform designed to protect the security, confidentiality and integrity of the information, data and other content, in any form,

that is provided, entered or uploaded by Client to the Platform ("**Client Data**"). The parties agree to the Data Processing Agreement set out in Attachment 2, attached hereto.

5.3 Client shall not, and shall ensure that its authorized users do not: (i) use the Platform to upload, transmit, or otherwise distribute any content that is threatening, defamatory, fraudulent, infringing, or otherwise unlawful; (ii) store, submit, or distribute viruses, worms, time bombs, malicious code, or any other items of a harmful nature; (iii) use the Platform for any unlawful purpose or to engage in any activity that violates applicable law or the rights of others; (iv) engage in any activity that interferes with or disrupts the Platform or third party data contained therein; (v) attempt to gain unauthorized access to the Platform or its related systems or networks; or (vi) make derivative works of, disassemble, or attempt to reverse compile or reverse engineer any part of the Platform or Services, or access the Platform in order to build a similar or competitive product or service (or contract with a third party to do so).

6. Ownership

6.1 Except for the rights expressly granted to Sterling in this Agreement, Client shall retain all right, title and interest to the Client Data. Notwithstanding the foregoing, Sterling may compile, extract or anonymize data from Client Data in connection with its performance of the Services in aggregate statistical form in such a way that neither the individual(s) being screened nor Client can reasonably be identified, and Sterling will own all right, title and interest in such compiled, extracted or anonymized data. Sterling shall retain all right, title and interest in and to the Platform and all technology and software used to provide it, including all modifications and/or enhancements to the Platform, regardless of the source of inspiration.

7. Disclaimers

7.1 Client acknowledges (a) that the depth of information collected by Sterling varies among sources and Sterling cannot act as an insurer or guarantor of the accuracy, reliability or completeness of the data, and (b) that the information that Sterling discovers with respect to the subject of a background check report is subject to the reporting limitations of the FCRA and other applicable law.

7.2 Sterling may from time to time offer information, guidance, forms, materials, and/or other content (including sample documents) for informational purposes ("Content"), which is not intended to and shall not constitute legal or professional advice, either express or implied. Client agrees not to rely on Sterling for (nor shall Sterling render) legal or professional advice. Client acknowledges and agrees that it is solely responsible for its legal and employment related decisions and will consult with its own legal counsel (at Client's discretion) regarding all employment law related matters, including but not limited to its legal obligations with respect to its procurement and use of the Services and Screening Reports.

7.3 EXCEPT AS EXPLICITLY SET FORTH IN THIS AGREEMENT, (A) THE PLATFORM, CONTENT AND ALL SERVICES ARE PROVIDED ON AN "AS IS," "AS AVAILABLE" BASIS, (B) STERLING DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND (C) STERLING DOES NOT WARRANT THAT THE PLATFORM, CONTENT OR SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE AND DISCLAIMS ANY WARRANTY OR REPRESENTATION REGARDING AVAILABILITY OF THE PLATFORM, SERVICES, SERVICE LEVELS OR PERFORMANCE.

8. Limitation of Liability

8.1 NEITHER PARTY WILL BE LIABLE FOR ANY INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY, INDIRECT, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOSS OF PROFITS), REGARDLESS OF WHETHER OR NOT THE OTHER PARTY WAS AWARE OR SHOULD HAVE BEEN AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

8.2. EACH PARTY'S MAXIMUM LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT, REGARDLESS OF THE CAUSE OF ACTION (WHETHER IN CONTRACT, TORT, BREACH OF WARRANTY OR OTHERWISE), WILL NOT EXCEED THE TOTAL AMOUNT PAID AND PAYABLE BY CLIENT HEREUNDER DURING THE 12-MONTH PERIOD IMMEDIATELY PRECEDING THE DATE ON WHICH SUCH LOSS, DAMAGE, INJURY, CLAIM, COST OR EXPENSE OCCURRED.

8.3. The foregoing limitations shall not apply to the extent not permitted by applicable law or with respect to breach of Sections 1.2, 1.3, 2.1, 3 or 4.1.

9. Termination

9.1 If a party materially breaches this Agreement, the non-breaching party may terminate this Agreement if such breach is not cured within sixty (60) days after written notice of such breach.

9.2 Sterling may immediately suspend Services or terminate this Agreement, in whole or in part, upon notice if (i) Client fails to pay amounts when due, (ii) Client files bankruptcy or reorganization or fails to discharge an involuntary petition within sixty (60) days after filing date, or (iii) Sterling reasonably believes that its provision, or Client's use, of the Services violates the FCRA or other applicable law.

9.3 All provisions that by their nature are intended to survive, including but not limited to payment obligations, disclaimers of warranties, confidentiality and limitations of liability, shall survive the termination of this Agreement.

10. Choice of Law; Disputes

10.1 This Agreement is governed by and construed in accordance with the laws of the State of New York, without regard to choice of law provisions. Any disputes arising out of this Agreement that cannot be resolved by the parties will be brought in state or federal court located in New York County, New York. The parties shall file in federal court when possible.

11. Miscellaneous

11.1 This Agreement, addenda, attachments, exhibits and/or schedules (including the Background Screening Requirements Addendum and Credentialing Application), constitute the entire agreement between Sterling and Client regarding the Services. All prior agreements, both oral and written, between the parties on the matters contained in this

Agreement are expressly cancelled and superseded by this Agreement. In no event shall any terms or conditions included on any form of Client purchase order apply to the relationship between Sterling and Client hereunder. In the event of any conflict between this Agreement and any addenda, attachments, exhibits and/or schedules, this Agreement shall control. Any amendments of or waivers relating to this Agreement must be in writing signed by the party, or parties, to be charged therewith. Except for Client's payment obligations hereunder, neither Party shall be responsible for any events or circumstances beyond its control including but not limited to war, riots, terrorism, embargoes, strikes and/or Acts of God) that prevent it from meeting its obligations under this Agreement. This Agreement may be executed in any number of counterparts, each of which will be deemed to be an original, and all of which taken together will be deemed to constitute one and the same instrument. Delivery of an executed signature page to this Agreement by any party by electronic transmission will be as effective as delivery of a manually executed copy of the Agreement by that party.

11.2 Except as otherwise set forth in this Agreement, all notices related to this Agreement shall be in writing and delivered to the party's address specified in this Agreement. Notices related to billing may be sent via electronic mail to the billing contact designated by Client.

11.3 Sterling shall provide notice (an alert via the Platform is sufficient) with respect to any change to or discontinuation of any Services and/or the Platform as necessary to comply with applicable law or vendor requirements.

11.4 Sterling may use Client's brands, logos, service marks, trade name, and other source identifiers for the purpose of representing to third parties that Sterling is providing Services to Client.

11.5 Neither party may assign this Agreement without the prior written consent of the other party; however, Sterling may assign this Agreement without prior written consent (i) to any of its affiliated companies, (ii) pursuant to a corporate reorganization, merger or consolidation of its business, or (iii) pursuant to the sale of all or substantially all of its assets.

11.6 Client acknowledges that Sterling's suppliers, vendors, and/or partners may require Client to execute additional terms and conditions and/or documentation as a condition precedent to Sterling providing certain services.

11.7 In connection with Sterling enforcing its rights under Sections 1.2, 1.3, and/or 2.1 of this Agreement, Sterling shall be entitled to recover all costs incurred, including reasonable attorneys' fees, in addition to any other relief to which it is entitled. The foregoing shall not be subject to the limitations set forth in Section 8 above.

	STERLING INFOSYSTEMS, INC.	**Client:**	
Signature:		**Signature:**	
Print Name:		**Print Name:**	
Title:		**Title:**	
Date:		**Date:**	

ATTACHMENT 1 – PRODUCTS AND PRICING

Client initial:

PLATFORM:

Expected Annual Volume (in number of applicants/employees searched) per Contract Year:

Unless otherwise noted in a product description, Client understands and acknowledges that the Services reflected herein may incur additional fees in accordance with the then-current Fee Schedule (available upon request and subject to change), including, without limitation, court access fees, employment/education third party database costs, out of network drug testing fees, and state Department of Motor Vehicle fees ("Fees"). Fees, if any, will be included on monthly invoices and are subject to change without notice.

Additional Services: The Platform includes an a la carte menu of select Sterling services ("Additional Services"). Unless already contracted for an Additional Service herein, all Additional Services will be available for Client to add to orders on a one-off basis at Sterling's then-current list price. The available Additional Services are subject to change without notice.

ATTACHMENT 2 – DATA PROCESSING AGREEMENT

1. Definitions

"**Agreement**" means the service agreement to which this DPA is attached.

"**Applicable Law**" means enactments that apply to the Processing of Client PI, including without limitation laws and regulations about privacy, data protection, police and court records, employment, and consumer reporting.

"**Authority**" means a court, regulatory or supervisory body, law enforcement agency or other government entity.

"**BCRs**" means binding corporate rules, as defined in the GDPR, which have been approved by the relevant Authority and apply to the Processing of Client PI by Sterling or a Subprocessor.

"**CCPA**" means the California Consumer Privacy Act (Cal. Civ. Code § 1798.100 et seq.).

"**Client Personal Information**" or "**Client PI**" means information about identified or identifiable individuals ("**Personal Information**" or "**PI**") Processed by Sterling under the Agreement.

"**Data Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Client PI in the custody of Sterling or a Subprocessor.[1]

"**Data Subject**" means an identified or identifiable individual.

"**European Adequate Protection Area**" means: (a) European Jurisdictions; (b) countries, or sectors within a specified country, that the European Commission (or other relevant Authority in a European Jurisdiction) recognizes as having an adequate level of protection for PI.

"**European Jurisdiction**" means any one of: (a) the European Economic Area ("EEA"); (b) Switzerland; or (c) the United Kingdom. [2]

"**European Law**" means the laws applicable in European Jurisdictions, including without limitation the General Data Protection Regulation (EU) 2016/679 ("GDPR").

"**FCRA**" means the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.).

"**GDPR Compensation Claim**" means a claim for compensation against a party under Article 82 GDPR and all compensation, legal fees and other expenses arising directly from that claim.

"**GDPR Fine**" means an administrative fine imposed against a party under Article 83 GDPR.

"**Process**" means to perform any operation on information, including without limitation collection, use, access, communication, disclosure, storage, destruction and Anonymization.

"**Programs**" means documented information security, privacy, disaster recovery and business continuity programs that include without limitation policies, procedures, training, testing, monitoring, and enforcement.

"**Retention Obligation**" means Sterling's obligation to retain Client PI under Applicable Law or a contract with a third-party source of Client PI. If Sterling is a data processor under European Law, then Retention Obligations are limited to those imposed by European Law.[3]

"**SCCs**" means the standard contractual clauses issued under European Commission Decision 2010/87/EU, or the relevant clauses issued to replace them.

"**Services**" means background screening or other services performed by Sterling under the Agreement.

---

[1] The GDPR definition of "personal data breach" is used here, as it is commonly accepted in many jurisdictions and covers the circumstances that would trigger an incident response around the world.

[2] These jurisdictions are grouped together because they have very similar data protection regimes which generally require similar steps to be taken when data is exported from the jurisdiction. The term is used to ensure that data leaving any one of the three discrete areas (the EEA, Switzerland, or the UK) will be treated in accordance with the rules of the exporting jurisdiction.

[3] In many jurisdictions, Sterling is independently obligated, by law or by contract, to retain personal information for a certain period to allow for audits or the exercise of data subject rights. Where Sterling is a data processor in Europe, Sterling is generally only entitled to retain personal information to comply with European law (and not with a contract or foreign law), so this definition is limited accordingly.

"**Subprocessor**" means an entity that Processes Client PI on behalf of Sterling.

"**Third-Party Request**" means a request, complaint, demand, notice or other communication Sterling receives from a Data Subject, Authority or other third party relating to Client's obligations under, or compliance with, Applicable law, other than communications that are necessary to provide the Services.

2. Compliance

2.1. The terms of this DPA will apply as long as Sterling or a Subprocessor has Client PI in its custody.
2.2. Sterling shall not authorize any person to Process Client PI unless that person is subject to appropriate confidentiality obligations.
2.3. Except as otherwise stated in this DPA, Sterling is responsible for Sterling personnel's and Subprocessors' compliance, and liable for their non-compliance, with this DPA and Applicable Law.
2.4. On Client's request and subject to any limitations set out in this DPA,[4] Sterling shall provide reasonable assistance to Client in meeting its data protection obligations under Applicable Law, taking into account the nature of the Processing and the information available to Sterling. This may include, without limitation, participation in security or data protection impact assessments, audits, and interactions with Data Subjects or Authorities.
2.5. Client shall not instruct Sterling to Process Client PI in violation of Applicable Law. If European Law applies, Sterling shall inform Client if Sterling believes any instruction from Client violates European Law.
2.6. Notwithstanding anything to the contrary in the Agreement or elsewhere, Sterling may deliver notice contemplated in this DPA by email or through its online platform.[5]

3. Roles of the Parties

3.1. For the purposes of European Law, the parties consider that Client is a controller and Sterling is a processor of Client PI, except as otherwise stated in this DPA or determined by an Authority.[6] For the purposes of federal or provincial privacy laws in Canada, the parties consider that Client has control of Client PI and Sterling has custody but not control of Client PI.
3.2. If Sterling is a responsible person or umbrella body for the purposes of criminal record disclosure carried out by the Disclosure and Barring Service, Disclosure Scotland or Access NI, then the parties consider that Sterling is a controller of Client PI Processed for these purposes.[7]
3.3. The parties acknowledge that Sterling's performance, and Client's use, of the Services are exempt from the CCPA to the extent they constitute the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a 'consumer reporting agency' or by a 'user' of a 'consumer report', as each of those terms is defined or used in the FCRA. If Sterling Processes Client PI relating to Data Subjects

[4] See most notably section 10, which sets out certain limitations on audit rights.

[5] The notices contemplated in the DPA are limited to Subprocessor updates (which are based on subscription and cannot comply with a formal notice procedure), and incident notifications, which are urgent and must be sent by email to the current business contact(s) who are most likely to be able to respond.

[6] Under the GDPR, a controller "establishes the purposes and means" for processing. Sterling does not establish the purposes for processing; we simply process data at our client's instruction. While our clients do generally delegate the detailed means of processing to Sterling, the essential means, namely: the selection of the service provider, the selection of the services, and the configuration of the services, is all done by our client. Several European data protection authorities have confirmed that this arrangement fits within the definition of a "processor", but the validity of the agreement would not be affected (and the way data is processed would not change) if a different authority decided otherwise.

[7] This is unique to Sterling's relationship with the criminal record disclosure authorities in the UK. Even if we are technically a 'controller' in these circumstances, the DPA still applies in its entirety and the way we process data remains the same. Note that these authorities are third-party controllers which set rules for access and use of information, and do not process data on behalf of Sterling or its clients.

who are California consumers (as defined in the CCPA) outside the context of this exemption ("**Non-FCRA Client PI**"), then the parties acknowledge that Sterling acts as a service provider for the purposes of the CCPA.[8]

3.4. Except as otherwise stated in this DPA or required by Applicable Law, Sterling shall: (a) notify Client of all Third-Party Requests without undue delay; (b) provide information and assistance to Client as Client reasonably requests to allow Client to respond to Third-Party Requests; and (c) not respond directly to Third-Party Requests except as directed by Client or required by Applicable Law.

4. Processing

4.1. This DPA applies to all Client PI that Sterling Processes. The types of Client PI that Sterling Processes that are subject to European Law, if applicable, are listed in Annex 2.[9]

4.2. The nature, purpose and subject matter of the Processing of Client PI are as documented in the Agreement.

4.3. The Data Subjects are Client's prospective or current employees, volunteers, tenants, students, members, directors, registrants, contractual partners or others as documented in the Agreement or a credentialing application completed by Client.

4.4. The duration of the Processing is the duration of the Agreement and thereafter according to any further documented agreement between the parties.

4.5. Client acknowledges that the nature of the Services may require disclosure of Client PI to, and collection of Client PI from, third parties that are not Subprocessors, including without limitation Authorities or the Data Subject's current and past employers or educational institutions. Client's request for Services will be deemed to be Client's instruction to Sterling to disclose Client PI to, and collect Client PI from, third parties that are not Subprocessors as necessary to perform those Services.[10]

4.6. Sterling shall not Process Client PI except as necessary to: (a) provide the Services as documented in the Agreement; (b) comply with Client's otherwise documented instructions, subject to the terms of the Agreement; or (c) comply with Applicable Law, provided Sterling has notified Client in advance of that Processing unless that notification is prohibited by Applicable Law.

4.7. Notwithstanding anything to the contrary in this DPA or the Agreement, if Sterling Processes Non-FCRA Client PI, then Sterling shall neither: (a) sell non-FCRA Client PI to any party other than Client; nor (b) retain, use or disclose Non-FCRA Client PI for any purpose other than for the specific purpose of performing the Services, or as otherwise permitted by the CCPA, including retaining, using or disclosing the Non-FCRA Client PI for a commercial purpose other than providing the Services.[11]

5. Subprocessing

5.1. Client hereby authorizes Sterling to use Subprocessors,[12] provided that: (a) Sterling shall maintain a complete and up-to-date list of Subprocessors at www.sterlingcheck.com/subprocessors[13] or another location as communicated by Sterling to Client from time to time; (b) Sterling shall sign a written agreement with each Subprocessor that imposes obligations on that Subprocessor that are no less stringent than those required of Sterling under Applicable Law, this DPA and Sterling's BCRs; and (c) Sterling will not be relieved of any of its obligations under this DPA or its BCRs by engaging Subprocessors.

5.2. The following only apply when Sterling uses Subprocessors to Process Client PI that is subject to European Law: (a) if Client notifies Sterling of an objection to Processing by a Subprocessor, Sterling shall not permit further Processing

---

[8] This exemption applies to all of Sterling's background screening services. The relevant provision of the CCPA can be found at subdivision 1798.145(d).

[9] The list at Annex 2 is intended to be exhaustive but can be amended as needed to reflect the intended use of our services.

[10] This is a factual statement of the nature of Sterling's services. Sterling acts as an intermediary between our client and third parties with which we have no relationship, but which have relationships with or otherwise may hold information about specific data subjects.

[11] This text comes directly from the CCPA and ensures that this contract is a valid "service provider" contract as set out in that law.

[12] Due to the large number of Subprocessors that Sterling uses, and the frequency with which they change, it is not possible to seek case-by-case approval for the use of Subprocessors.

[13] This site is password protected, but the password can be obtained at any time by emailing privacy@sterlingcheck.com.

of Client PI by that Subprocessor; (b) Client's objection to Processing by a Subprocessor will be deemed to be Client's waiver of Sterling's obligation to perform Services that Sterling would ordinarily perform using that Subprocessor;[14] (c) if Sterling adds or replaces a Subprocessor, Sterling shall notify Client (subject to Client's subscription to those notifications at the form co-located with the list of Subprocessors) of the addition or replacement at least 30 calendar days before the new Subprocessor begins Processing Client PI; and (d) notwithstanding the other provisions in this section, Sterling may add or replace a Subprocessor immediately upon notice to Client if it is necessary to ensure business continuity and recovery in case of emergency, except as prohibited by Applicable Law.

6. Cross-Border Data Transfers

6.1. Sterling and Client shall cooperate to ensure that appropriate notice to Data Subjects and safeguards or other legal mechanisms for cross-border data transfers are in place as required by Applicable Law.[15]

6.2. If Sterling Processes Client PI that is subject to European Law and transfers that Client PI to a Subprocessor outside the European Adequate Protection Area, then Sterling shall either: (a) ensure that BCRs apply to that transfer; or (b) sign SCCs with that Subprocessor for Client's benefit.[16]

6.3. If the nature of the Services require Sterling to transfer Client PI that is subject to European Law to a third party that is not a Subprocessor outside of the European Adequate Protection Area, then Sterling shall only transfer that Client PI upon Client's documented instruction. Client's request for Services that require such a transfer, for example to collect or verify information about a Data Subject's current or past residence, education or professional activities outside of the European Adequate Protection Area, will be deemed to be Client's documented instruction for that transfer. Unless Client determines that another mechanism or derogation under European Law applies, Sterling and Client shall cooperate to obtain the Data Subject's prior explicit and informed consent for transfers described in this section.[17]

7. Security Controls

7.1. Sterling shall implement, maintain and enforce Programs that contain appropriate administrative, technical and physical measures designed to protect the security, integrity, confidentiality and availability of Client PI and protect Client PI against a Data Incident, considering the likelihood and severity of a potential Data Incident. Sterling shall review and, if appropriate, update these measures periodically to comply with Applicable Law. Sterling shall regularly test these measures for effectiveness.

7.2. General information about the Programs at the Effective Date is in Annex 1. Sterling shall provide detailed documentation of the Programs to Client on request and shall not materially degrade the level of protection set out in the Programs.

---

[14] In many instances, only one subprocessor can be used to conduct a service, especially when a local presence or specialized skill is required. For that reason, an objection to a subprocessor in many cases will render the services impossible to perform. As Sterling generally bills for services after they are rendered, the waiver of Sterling's obligation necessarily means that no payment obligation will arise.

[15] Where notice to a data subject is required for a cross-border transfer, Sterling cannot independently guarantee that this will be carried out, as we do not always have an interaction with the data subject. However, we will cooperate to achieve this by making sample notices available and providing necessary information to our client. Note that in many jurisdictions, including the United States, there are few or no formalities required for cross-border data transfers.

[16] Certain subprocessors (like Salesforce.com) have received regulatory approval for their own intra-group data transfer mechanism, known as BCRs. Sterling has also applied for BCR approval within its own corporate group. In all other cases where data is transferred to a subprocessor (either a Sterling affiliate or an unaffiliated third party) outside of a European jurisdiction and there is no applicable adequacy decision, Sterling will sign SCCs with that subprocessor.

[17] Sterling's services involve interactions with third parties with which we have no relationship, as they are associated with the data subject, not with Sterling. In such cases, there is no reasonable way to ensure there are safeguards for cross-border data transfers as set out in European data protection laws. This is usually the case when an applicant for work in Europe has past residence, work or education history outside of Europe. In these cases, our clients generally rely on the consent of the data subject for the transfer.

8. Data Incidents

8.1. Sterling shall implement and maintain a Data Incident response protocol and provide documentation of that protocol to Client on request.

8.2. In the event of a Data Incident, Sterling shall notify Client without undue delay, and in any event within a timeline that permits Client to comply with its legal obligations,[18] and take all reasonable steps to investigate and resolve the Data Incident and provide a comprehensive report to Client on that investigation and resolution.

8.3. If Applicable Law requires notification of a Data Incident to Authorities or Data Subjects, or provision of any remediation services including without limitation credit or identity monitoring, then Sterling shall, where permitted by Applicable Law, carry out that notification or provide those services if either of the following is true: (a) Client instructs Sterling to do so; or (b) Sterling notifies Client that it intends to do so, gives Client a reasonable opportunity to object, and Client does not object.[19]

8.4. Sterling shall bear the costs of investigation, notification and remediation services that Sterling carries out, procures or provides, except to the extent that the Data Incident is caused or aggravated by Client's act or omission.

9. Data Retention and Destruction

9.1. Client hereby instructs Sterling to retain Client PI as necessary to comply with its Retention Obligations. Sterling shall provide details of its Retention Obligations to Client on request.[20]

9.2. Once Retention Obligations are met, subject to the delay required to comply with section 9.4, Sterling shall delete Client PI upon the earlier of either: (a) Client's instruction; or (b) termination or expiration of the Agreement. On Client's request, Sterling shall certify in writing to Client that it has deleted Client PI.

9.3. Notwithstanding anything to the contrary in this DPA or the Agreement, the parties agree that Sterling does not intend, and makes no guarantee, to retain Client PI for more than seven years after the date Sterling received it. Client hereby authorizes Sterling to delete Client PI after that time has passed.[21]

9.4. Upon termination or expiration of the Agreement or before Sterling deletes Client PI, whichever is earlier, Sterling shall, either: (a) give Client a reasonable opportunity to retrieve Client PI from Sterling's systems; or (b) provide Client PI to Client in a machine-readable format, subject to additional charge at Sterling's discretion if permitted by law.

10. Audit and Inspection

10.1. On Client's request, Sterling shall make available to Client all information reasonably necessary to demonstrate Sterling's compliance with this DPA, the Programs and Applicable Law.

10.2. Client or another party of Client's choosing may conduct an audit of Sterling's compliance with this DPA, the Programs and Applicable Law, provided that: (a) Client shall not request more than one audit per calendar year, except as otherwise stated in this DPA; (b) Client shall give Sterling reasonable notice of an audit, shall ensure that the audit is conducted at a mutually agreeable time, and shall ensure that the audit does not unreasonably interfere with Sterling's operations; and (c) access to Sterling's facilities and confidential information will be subject to Sterling's policies and reasonable confidentiality provisions.

10.3. If, during an audit, Client discovers non-compliance with this DPA, the Programs or Applicable Law, Client and Sterling shall work in good faith to agree on a remediation plan, which Sterling shall carry out.

10.4. Subject to the requirements and limitations in 10.2(b) and 10.2(c), Client may conduct: (a) one additional audit in each calendar year in response to each Data Incident; and (b) additional audits as may be reasonably necessary to comply with Applicable Law or the order of an Authority.

10.5. Each party shall bear its own expenses in conducting or participating in an audit.

---

[18] While we understand that some of our clients prefer to put in place a specific timeline for incident notification, in reality it is impossible to guarantee we will meet such a timeline due to the number of clients we have and the complexity of our business. For that reason, we can only commit to notification without undue delay (the standard set by the GDPR) and in any event we guarantee that any delay in notification on our side will not interfere with our client's ability to comply with the law.

[19] As a large-scale incident is likely to affect more than one of Sterling's clients, Sterling must be able to conduct a centralized incident response and notification effort. However, we engage our client before notifying individuals.

[20] Retention obligations are dependent on services ordered and can change; for that reason, they are not listed here. They generally exist in North America only and do not exceed six years.

[21] Sterling does not offer long-term data storage services. For that reason, we cap data retention at seven years.

11. Data Subjects' Rights

11.1. Client shall provide a notice or disclosure to, and, if necessary, collect consent or authorization from Data Subjects for the transfer of Client PI to Sterling and the Processing of Client PI by Sterling as required by Applicable Law.[22] Sterling may make available to Client its systems or sample text for these purposes. Client acknowledges that its use of Sterling's systems or sample text does not relieve Client of its responsibility for compliance with notice, disclosure, authorization and consent provisions in Applicable Law.

11.2. Sterling shall respond to Data Subjects who communicate with Sterling directly or are referred to Sterling by Client to: (a) inquire about PI in Sterling's custody; (b) inquire about Sterling's Processing of PI; or (c) exercise the Data Subject's rights to access or rectify PI in Sterling's custody. Sterling shall respond to these communications in accordance with Applicable Law. Sterling shall inform Client of the existence, content, and handling of these communications on Client's request.

12. GDPR Liability[23]

12.1. Notwithstanding any limitation of liability provisions in the Agreement,[24] each party shall indemnify the other party against a GDPR Compensation Claim in accordance with the indemnifying party's part of responsibility for the damage giving rise to the GDPR Compensation Claim,[25] subject to the following: (a) the party seeking indemnification must notify the indemnifying party without undue delay upon becoming aware that a GDPR Compensation Claim has been or may be made; (b) the party seeking indemnification must take all reasonable measures to minimize the risk, and amount, of a GDPR Compensation Claim; and (c) the party seeking indemnification must reasonably cooperate with the indemnifying party to defend against or otherwise respond to the GDPR Compensation Claim in a mutually acceptable way.

12.2. If either party is held liable, individually or jointly with a third party, for a GDPR Fine, then that party shall ensure that fine is paid and shall not seek, and will not be entitled to recover, indemnity from the other party, notwithstanding any provision to the contrary in the Agreement or this DPA.[26]

---

[22] While Sterling can assist in some cases with the administrative service of providing notice or collecting consent, use of those administrative services is optional and the legal obligation to provide notice and collect consent remains with our client.

[23] Liability in case of data incident expenses is covered at section 8.4. Liability under articles 82 and 83 of the GDPR is unique, and is treated so here. All other liability related to privacy or data protection is covered under the service agreement.

[24] European regulators recommend against any contractual provision which would have the effect of limiting liability towards a data subject.

[25] Article 82 of the GDPR states that multiple parties involved in data processing may be held jointly and severally liable to the data subject, regardless of fault; it is then incumbent on the parties to work out responsibility among themselves.

[26] Fines under Article 83 of the GDPR can only be issued against a party based on its own infringement of the law. Sterling cannot assume responsibility for its client's infringement of the law, nor do we ask for our clients to assume responsibility for ours.

ANNEX 1 – INFORMATION SECURITY, PRIVACY, DISASTER RECOVERY AND BUSINESS CONTINUITY PROGRAMS

Sterling shall, as a minimum, implement the following types of security measures, and shall update those measures in accordance with industry best practice.

Access control to premises and facilities

Measures in place to prevent unauthorized physical access to premises and facilities holding Personal Information:

- Locked doors;
- Access control system using electronic access, biometric access or physical key;
- Alarm system;
- Video surveillance;
- Logging of facility exits/entries.

Access control to systems

Measures in place to prevent unauthorized access to IT systems:

- Password procedures (including minimum length and complexity, and forced change of password);
- No access for guest users or anonymous accounts;
- Central management of system access;
- Access to IT systems subject to approval from HR management and IT system administrators;
- Full suite of firewall controls monitoring inbound and outbound traffic against a pre-established set of permissible traffic flows;
- Intrusion detection and prevention capabilities monitoring inbound traffic for malicious patterns and traffic anomalies;
- Ability to detect and respond to direct and distributed denial of service attacks through network routing and DNS controls;
- All application deployments subject to automated security testing against Open Web Application Security Project (OWASP) Top-Ten list to ensure adequate protection against common web application attacks;
- All hosts run anti-malware solutions with advanced persistent threat detection capabilities performing real-time behavior analysis of machine and network behavior. The presence of this software is required to join the network through network access control;
- All end-user devices participate in a network access control mechanism which requires hosts to be pre-authorized and authenticated to the network and ensures that hosts are running the minimum set of information security controls prior to be granted access.

Access control to data

Measures in place to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorized input, reading, copying, removal, modification or disclosure of data:

- Differentiated access rights;
- Access rights defined according to duties;
- Automated log of user access via IT systems;
- Measures to prevent the use of automated data-processing systems by unauthorized persons using data communication equipment;
- All remote access to internal corporate network and consoles requires multi-factor authentication through a VPN tunnel from a pre-authorized machine;
- All hosts are running host-based data loss prevention software monitoring for the movement of sensitive data to and from the host. The presence of this software is required to join the network through network access control;
- All databases containing sensitive information are required to be encrypted to protect against theft or loss of database files.

Disclosure control

Measures in place to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged:

- Compulsory use of a wholly-owned private network for all data transfers within the corporate group;
- All end-user devices are required to be full-disk encrypted to protect against data incidents through theft or loss. The presence of this software is required to join the network through network access control;
- Prohibition of portable media;
- Creating an audit trail of all data transfers.

Input control

- Measures in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained:
- Logging user activities on IT systems;

- Ensuring that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment;
- Ensuring that it is possible to verify and establish which personal data have been entered into automated data-processing systems and when and by whom the data have been entered.

Job control

Measures in place to ensure that data is processed strictly in compliance with the controller's instructions:

- Unambiguous wording of contractual instructions;
- Monitoring of contract performance.

Availability control

Measures in place to ensure that data are protected against accidental destruction or loss:

- Ensuring that installed systems may, in the case of interruption, be restored;
- Ensuring systems are functioning, and that faults are reported;
- Ensuring stored personal data cannot be corrupted by means of a malfunctioning of the system;
- Uninterruptible power supply (UPS);
- Business Continuity procedures;
- Remote storage;
- Anti-virus/firewall systems.

Segregation control

Measures in place to allow data collected for different purposes to be processed separately:

- Restriction of access to data stored for different purposes according to staff duties;
- Segregation of business IT systems;
- Segregation of IT testing and production environments.

Audit

Measures in place to ensure proper functioning of controls:

- Audited and certified each year to the ISO 27001:2013 standard in multiple locations throughout the world;
- Audited and certified by the National Association of Professional Background Screeners (NAPBS) for compliance, quality, and security;
- Has submitted documentation and obtained certification to the UK Cyber Essentials standard;
- Audited multiple times throughout the year by external clients as part of their own internal risk management processes;
- Audited multiple times each year through internal risk management processes by internal audit teams for application security, vulnerability assessments, and network security.

ANNEX 2 – TYPES OF CLIENT PERSONAL INFORMATION

Sterling may Process the following types of Client Personal Information under the Agreement:

- Identification information
- Copies of identity documents
- Phone and email contact information
- Current and past addresses and proof of address
- Right to work, immigration status and work permit information
- Education history and qualifications
- Employment or volunteering history, including, where applicable, fiduciary or directorship responsibilities
- Gap or travel activities
- Personal and Professional references
- Professional qualifications and registrations with professional bodies
- Publicly sourced information (e.g. media or online information)
- Driver's license and status, including driver history and expiration date
- Opinions about Data Subjects from references they have provided
- Civil court records
- Government-issued or financial identification numbers
- Date of birth
- Sanctions with professional bodies
- Financial information such as credit history, bankruptcy, financial judgments or tax information

Sterling may also Process the following types of Client Personal Information that may be considered "sensitive" or "special categories" under European Law:

- Place of birth
- Sex
- Criminal history
- Appearance on global sanctions or terrorist watch lists
- Driving records, penalties and restrictions

BACKGROUND SCREENING REQUIREMENTS ADDENDUM (FCRA)

In connection with the Service Agreement ("Agreement") by and between Sterling Infosystems, Inc. dba Sterling ("Sterling") and ("End User" or "Client"), Sterling will furnish End User with Screening Reports conditioned upon End User's compliance with its obligations set forth below (and in the Agreement). This Background Screening Requirements Addendum (this "Addendum") is incorporated into and made part of the Agreement. Capitalized terms used but not defined in this Addendum shall have the meanings ascribed to them in the Agreement.

1. **FCRA Certification**. To the extent that End User is located in the United States and/or End User's procurement and/or use of Screening Reports is subject to the Fair Credit Reporting Act ("FCRA"), End User certifies that it will do the following:

1.1. **Permissible Purpose**. Pursuant to the FCRA (15 U.S.C. § 1681b(a)(3)(B)), End User hereby certifies that all of its orders for Screening Reports from Sterling shall be made, and the resulting reports shall be used for employment purposes, as defined in the FCRA, including evaluating a consumer for employment, promotion, reassignment or retention as an employee, where the consumer has given prior written permission.

1.2. **Equal Employment Opportunity.** Pursuant to the FCRA (15 USC 1681b(b)(1)(A)(ii)), End User further certifies that information from any Screening Report will not be used in violation of any applicable federal or state equal opportunity law or regulation.

1.3. **Receipt of Required Notices**. Pursuant to the FCRA (15 USC 1681e(d) and 15 USC 1681b(b)(1)(B)), End User acknowledges that it has received and reviewed a copy of the notices titled (i) *Notice to Users of Consumer Reports: Obligations of Users Under the Fair Credit Reporting Act ("Notice to Users"),* which explains End User's obligations under the FCRA as a user of consumer information and a copy of which is attached hereto as Exhibit A-1, and (ii) *A Summary of Your Rights Under the Fair Credit Reporting Act*, a copy of which is attached hereto as Exhibit A-2**.** End User certifies that it will comply with all applicable provisions of Notice to Users.

1.4. **Disclosure and Authorization**. Pursuant to the FCRA (15 USC 1681b(b)(1)(A)(i)), End User agrees and certifies that prior to procurement or causing the procurement of a consumer report for employment purposes: (a) A clear and conspicuous disclosure has been made in writing to the consumer, in a document that consists of only the disclosure, explaining that a consumer report may be obtained for employment purposes and such disclosure satisfied all of the requirements of the FCRA as well as any applicable state or local laws; and (b) The consumer has authorized in writing the procurement of the report by End User.

1.5. **Investigative Consumer Reports**. Pursuant to the FCRA (15 USC 1681d(a)(2)), in addition to the disclosure and authorization requirements in Section 1.4 above, End User agrees and certifies that prior to procurement or causing the procurement of an investigative consumer report for employment purposes: (a) It has been clearly and accurately disclosed to the consumer that an investigative consumer report including information as to the consumer's character, general reputation, personal characteristics and/or mode of living may be made; and (b) Such disclosure (i) is made in a writing mailed, or otherwise delivered, to the consumer, not later than three days after the date on which the report was first requested, (ii) contains a statement informing the consumer of his/her right to request a complete and accurate disclosure of the nature and scope of the requested investigation and his/her right to request a copy of the rights of the consumer under the FCRA titled *A Summary of Your Rights Under the Fair Credit Reporting Act*, and (iii) satisfied all of the requirements of the FCRA as well as any applicable state or local laws. If the consumer makes a request within a reasonable time after his/her receipt of the required disclosure, End User certifies that it shall make a complete and accurate disclosure of the investigation requested. Such disclosure shall be made in a writing mailed, or otherwise delivered, to the consumer not later than five (5) days after the date on which the request for such disclosure was received from the consumer or such report was first requested, whichever is the later.

1.6. **Adverse Action**. Pursuant to the FCRA (15 USC 1681b(b)(1)(A)(i)), before taking any adverse action based in whole or in part on a Screening Report, End User must adhere to certain obligations. At a minimum, in using a Screening Report for employment purposes, before taking any adverse action based in whole or in part on the Screening Report, End User shall provide to the consumer to whom the Screening Report relates: (a) A pre-adverse action notice/letter stating that End User is considering taking adverse action; (b) A copy of the full and complete Screening Report; (c) A copy of the notice titled *A Summary of Your Rights Under the Fair Credit Reporting Act* and any applicable state summary of rights; (d) A reasonable opportunity of time to correct any erroneous information contained in the Screening Report; and (e) Contact information for Sterling. If End User thereafter takes adverse action, End User shall also provide a final adverse action notice to the consumer to whom the Screening Report relates. Such notice shall comply with all applicable laws, and shall include the name, address, and phone number of Sterling; a statement that Sterling did not make the decision to take the unfavorable

action and cannot give specific reasons for it; and a notice of the person's right to dispute the accuracy or completeness of any information Sterling furnished, and to get an additional free report from Sterling if the person asks for it within 60 days.

1.7. **Continuing Certification.** End User certifies that each and every time it requests a Screening Report regardless of ordering mechanism, it is at the time that the order is placed reaffirming its certifications herein, including without limitation, Section 1.4 above.

1.8. **Required Certification Updates.** If Sterling determines, in Sterling's sole discretion, that regulatory or industry changes require updates to the Employer Certification in this Section 1, Sterling retains the right to request and require additional documentation and certifications from End User. End User understands that any failure to cooperate with reasonable requests for such documentation and certifications may constitute grounds for immediate suspension of the Services and termination of the Agreement.

2. State Certifications.

2.1. **California Certification**. End User hereby certifies that, under the Investigative Consumer Reporting Agencies Act ("ICRAA"), California Civil Code Sections 1786 et seq., and the Consumer Credit Reporting Agencies Act ("CCRAA"), California Civil Code Sections 1785.1 et seq., to the extent End User is located in the State of California, and/or End User's request for and/or use of Screening Reports pertains to a California resident or worker, End User will do the following:

2.1.1. Request and use Screening Reports solely for permissible purpose(s) identified under California Civil Code Sections 1785.11 and 1786.12.

2.1.2. Pursuant to the ICRAA (Cal. Civ. Code § 1786.16(a)(2)(B)), when, at any time, a Screening Report is 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: (i) that an investigative Screening Report may be obtained; (ii) the permissible purpose of the investigative Screening Report; (iii) that information on the consumer's character, general reputation, personal characteristics and mode of living may be disclosed; (iv) the name, address, and telephone number of Sterling; and (v) the nature and scope of the investigation requested, including a summary of the provisions of California Civil Code Section 1786.22.

2.1.3. Pursuant to the ICRAA (Cal. Civ. Code § 1786.16(a)(2)(C)), when, at any time, a Screening Report is sought for employment purposes other than suspicion of wrongdoing or misconduct by the consumer who is the subject of the investigation, only request a Screening Report if the applicable consumer has authorized in writing the procurement of the Screening Report.

2.1.4. Pursuant to the ICRAA (Cal. Civ. Code § 1786.16(b)(1)), 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 Screening Report that is prepared.

2.1.5. Pursuant to the ICRAA (Cal. Civ. Code § 1786.16(b)(1)), if the consumer wishes to receive a copy of the Screening Report, send (or contract with another entity to send) a copy of the Screening Report to the consumer within three business days of the date that the Screening Report is provided to End User. The copy of the Screening Report shall contain the name, address, and telephone number of the person who issued the report and how to contact him/her.

2.1.6. Pursuant to the ICRAA (Cal. Civ. Code § 1786.16(b)(2)), 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 Screening Report, informing the consumer in writing of Sterling's name, address, and telephone number, and provide the consumer with a written notice of his/her rights under the ICRAA and the CCRAA.

2.2. **Vermont Certification**. In addition to the *Notice to Users*, if End User is a user of Vermont Screening Reports, End User certifies that it will comply with the applicable provisions of Vermont law, including, without limitation, Section 2480e of the Vermont Fair Credit Reporting Statute. End User further certifies that it has received a copy of Section 2480e of the Vermont Fair Credit Reporting Statute, attached hereto as Exhibit A-3.

3. General Use Requirements. End User further agrees that:

3.1. It will use each Screening Report only for a one-time use.

3.2. It shall provide access to Screening Reports provided by Sterling only to employees, agents and representatives of End User who fully review and understand End User's obligations under the FCRA and the Agreement and who agree to comply with those obligations.

3.3. It shall ensure that its users do not request and/or obtain Screening Reports on themselves, coworkers, employees, family members or friends unless it is in connection with a legitimate business transaction and procured in accordance with the terms of this Addendum.

3.4. End User shall dispose of any Screening Reports and any other documentation containing personally identifiable information received from Sterling in accordance with applicable law, including without limitation, the FACTA Disposal Rules.

3.5. End User shall implement and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to the End User's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to End User by Sterling; and that such safeguards shall be reasonably designed to (i) ensure the security and confidentiality of the information provided by Sterling, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer.

3.6. It has the obligation to make available to Sterling upon request copies of written authorizations and disclosures and any reports for a period of six (6) years.

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

4. Product-Specific Requirements.

4.1. **SSN Trace and Death Master File.** If Screening Reports include Social Security Number Trace ("SSN Trace") or the Death Master File search, End User shall not use Social Security Number trace results or the Death Master File search, in any way, directly or indirectly, for the purpose of making employment or other FCRA decisions. End User also confirms that it will not use Social Security Number trace information or the Death Master File search, in any way that would violate the privacy obligations or any other terms and provisions of the Gramm–Leach-Bliley Act (15 U.S.C 6801 et seq.) or the Federal Drivers Privacy Protection Act (18.U.S.C. Section 2721 et seq.) or any other similar U.S. state or local statute, rule or regulation.

4.2. **U.S. MVRs.** If Screening Reports include United States motor vehicle reports ("MVRs"), End User:

4.2.1. Shall comply with the Drivers Privacy Protection Act ("DPPA") and any applicable state laws.

4.2.2. Shall be responsible for understanding and for staying current with all specific state forms, certificates of use or other documents or agreements including any changes, supplements or amendments thereto imposed by the states (collectively referred to as "Specific State Forms") from which it will order MVRs. End User certifies that it will file all applicable Specific State Forms required by individual states.

4.2.3. Certifies that no MVRs shall be ordered without first obtaining the written consent of the data subject to obtain "driving records," evidence of which shall be transmitted to Sterling in the form of the data subject's signed release authorization form. End User also certifies that it will use this information only in the normal course of business (i) to obtain lawful information relating to the holder of a commercial driver's license, or (ii) to verify information provided by a candidate or employee. End User shall protect the privacy of the information of the data subject in an MVR and shall not transmit any data contained in the resulting MVR via any unsecured means.

4.3. **Massachusetts iCORI.** To the extent End User is requesting Sterling to provide Massachusetts iCORI information: (i) End User notified the consumer in writing of, and received permission via a separate authorization for Sterling to obtain and provide CORI information to End User; (ii) End User is in compliance with all federal and state credit reporting statutes; (iii) End User will not misuse any CORI information provided in violation of federal or state equal employment opportunity laws or regulations; and (iv) End User will provide Sterling with a statement of the annual salary of the position for which the subject is screened.

4.4. **Credit Reports.** If Screening Reports include credit reports, End User**:**

4.4.1. Certifies that it will promptly notify Sterling of any change in its location, structure, ownership or control, including but not limited to the addition of any branch(es) that will be requesting and/or accessing credit reports.

4.4.2. Acknowledges and understands that credit bureaus may prohibit the following persons, entities and/or businesses from obtaining credit reports: adult entertainment service of any kind; asset location service; attorney or law firm engaged in the practice of law (unless engaged in collection or using the report in connection with a consumer bankruptcy pursuant to the written authorization of the consumer); bail bondsman (unless licensed by the state in which they are operating); child location service – company that locates missing children; credit counseling (except not-for-profit credit counselors); credit repair clinic; dating service; financial counseling (except a registered securities broker dealer or a certified financial planner); with respect to U.S. credit reports, foreign company or

agency of a foreign government; genealogical or heir research firm; law enforcement agency; massage service; news agency or journalist; pawn shop; private detective, detective agency or investigative company; repossession company; subscriptions (magazines, book clubs, record clubs, etc.); tattoo service; time shares - company seeking information in connection with time shares (exception: financers of time shares); weapons dealer, seller or distributor.

5. **Right to Audit.** End User agrees to cooperate with any reasonable audit request by Sterling and/or a third-party data supplier of Sterling to assure compliance with the terms of this Addendum; provided that (i) Sterling shall give End User reasonable prior notice of any such audit; (ii) any such audit shall be subject to End User's security policies and third-party confidentiality obligations, and (iii) Sterling shall conduct or cause to be conducted such audit in a manner designed to minimize disruption of End User's normal business operations. End User understands that any failure to cooperate with reasonable requests regarding an audit constitutes grounds for immediate suspension of the Services and termination of the Agreement.
6. **Hold Harmless.** End User agrees to indemnify and hold harmless Sterling, its suppliers, and their successors and assigns, and their current and former officers, directors, employees, and agents, both individually and in their official capacities from any liability and attorneys' fees incurred due to End User's violation of any of the terms of this Addendum or failure to comply with applicable law.

Client:	
Signature:	
Print Name:	
Title:	
Date:	

EXHIBIT A-1

All users of consumer reports must comply with all applicable regulations. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

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

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's (CFPB) website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at 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 identify theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

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

F. Users Have Obligations When Disposing of Records

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

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

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

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

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

A. Employment Other Than in the Trucking Industry

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

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

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

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

B. Employment in the Trucking Industry

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

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

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

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

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

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

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used

for employment purposes – or in connection with a credit transaction (except as provided in federal regulations) – the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or a permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(1), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain 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 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 identify of all end-users;
(2) certifications from all users of each purpose for which reports will be used; and
(3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

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

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

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1618 et seq.:

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

EXHIBIT A-2

Para información en español, visite www.consumerfinance.gov/learnmore o escribe a la Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

A Summary of Your 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 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 identity 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 form 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).

- The following FCRA right applies with respect to nationwide consumer reporting agencies**:**

  CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

  You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

  As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

  A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

- **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, N.W. Washington, DC 20552 b. Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. 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 Financial Protection (OCFP) Division of Consumer Compliance Policy and Outreach 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, S.E. Washington, DC 20590
4. Creditors Subject to the Surface Transportation Board	Office of Proceedings, Surface Transportation Board Department of Transportation 395 E Street, S.W. Washington, DC 20423
5. Creditors Subject to the 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, S.W., Suite 8200 Washington, DC 20416
7. Brokers and Dealers	Securities and Exchange Commission 100 F Street, N.E. 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	Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. Washington, DC 20580 (877) 382-4357

EXHIBIT A-3

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 Federal Trade Commission.

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.