User Name: Account #

SOUTH CAROLINA
DEPARTMENT OF MOTOR VEHICLES

PERSONAL INFORMATION MEMORANDUM OF AGREEMENT
WITH A SISTER STATE AGENCY
EMPLOYER NOTIFICATION PROGRAM DATA

This agreement is entered into between the Employer Notification Customer _____ ("User") and the South Carolina Department of Motor Vehicles, ("SCDMV"). The agreement will commence on the date it has been signed by both parties and will terminate in accordance with the termination or modification clauses as stated in this agreement. Notwithstanding termination, User remains subject to continuing obligations with regard to certain retained data as stated in this agreement.

WHEREAS, the User requests access to specific information that the SCDMV routinely collects and stores in the course of its regular business operations, solely for the purposes of the Employer Notification Program as provided in this agreement; and

WHEREAS, some, if not all, of the desired information is of a personal nature, which the User understands to mean any information that identifies or describes an individual including, but not limited to, an individual's name, home address (excluding zip code), date of birth, driver identification number, customer number, height, weight, race, and other physical details; and

WHEREAS, subject to the User's certification of its compliance with all applicable statutes and regulations, the SCDMV will provide requested information to the User subject to the conditions set forth herein.

The User certifies that it is entitled to obtain and use personal information contained in the SCDMV's data in accordance with the Driver Privacy Protection Act (DPPA), 18 U.S.C. Chapter 123. In particular, the User claims that its use of such personal data will fit the exemption of 18 U.S.C. §2721(b)(13), which states, "For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains." The User certifies that the information from said records will not be used for any purpose other than the purpose for which it is furnished.

The User certifies that it will comply with all applicable Federal and State statutes and regulations pertaining to personal information disseminated by the SCDMV which include but are not limited to the following: DPPA, 18 USC §§ 2721 *et seq*.; and privacy provisions enacted by the State of South Carolina, including S.C. Release of Licensing and Registration Information Laws SC Code §§56-3-510 to -540, the S.C. Freedom of Information Act S.C. Code §§30-4-160, *et seq*.; and the S.C. Family Privacy Protection Act (FPPA), S.C. Code §§30-2-10, *et seq*. And, specifically, S.C. *Code Ann.* §§30-2-50, a part of the FPPA, requires the SCDMV to give notice to all requestors of records that obtaining or using public records for commercial solicitation directed to any person in this State is prohibited.

1. OBLIGATIONS OF THE PARTIES

The User and the SCDMV hereby enter into this agreement by which the User will obtain certain information and/or documents from the SCDMV's records for the purpose of monitoring employee driving records. The SCDMV agrees to make available the information, data, and/or documents requested by the User about the SCDMV's customers, to be accessed by the User via web-based services. There is no cost for this service to User.

The service the SCDMV will provide is SCDMV's Employer Notification Program. This service is a web-based employee monitoring application that provides updated driver information weekly about the User's employees as designated by User. User will only designate its actual employees and will only seek driver information for its own employees. The information available via this service will be for a 12-month calendar period.

The web-based application can be found at SCDMV's website:
https://www.scdmvonline.com/SCTRNS/Member/Logon.aspx

Prior to gaining access to the web-based application, User agrees to:

a.) receive, securely store, account for, and be fully responsible for all records received from the SCDMV.
b.) designate in this agreement a User Security Administrator ("SA") who will be provided SCDMV Administrator Account through which the SA will be responsible for maintaining the accounts of all User's authorized personnel who have authorized access to SCDMV data by the creation of an SCDMV Administrator Account ("Accessing User"). The Account will allow the Security Administrator "SA" to create and maintain Accessing User accounts for SCDMV Driver data access. This access is limited to User's employees assigned to jobs needing Driver Inquiries in order to carry out their official governmental duties.
c.) not retain or provide hard copy prints of personal information obtained from SCDMV records via the Inquiry web screens to any external customers and only to User's staff whose official job responsibilities require them to verify driver record information. The User recognizes that any information printed from SCDMV records does not retain currency after it is printed.
d.) ensure that an individual seeking access must also acknowledge familiarity with the requirements of this contract and applicable personal privacy rules and statutes as detailed in this agreement. User agrees to provide and document security awareness training for all employees/personnel with access to SCDMV data. As a minimum, this training must emphasize the importance of protecting customer private information, including Personally Identifiable Information (PII), against unauthorized disclosure. Training must also stress protecting passwords and accounts providing access to the SCDMV data. Emphasis will be placed upon the use of strong, non-dictionary passwords containing a combination of at least eight upper- and lower-case letters, at least one

special character, and at least one number. Emphasis must be placed upon not sharing passwords.

e.) ensure that the User SA must keep a current list of the personnel authorized to use these screens and must be responsible for account maintenance (resetting Accessing User id/passwords, deleting accounts for employees who are terminated, creating new accounts, and so forth). The User must immediately delete or remove access to any authorized Accessing User whose employment with the User is terminated for any reason.

f.) permit the User SA to authorize access only within the scope of actual need. The User shall not authorize the printing or distribution of screenshots of User information to employees who have not been authorized access to the SCDMV's information. The User will likewise ensure that the screenshots, if printed or retained in any form, are not placed in files accessed by employees who have not been authorized access to the SCDMV's information.

g.) require persons requesting authorized access to SCDMV data to agree in writing that neither the account nor passwords nor User ids/passwords related to the account may be shared with any other person or employee other than the approved Accessing Users.

h.) let User's Authorized Officer's signature below, serve as verification and acknowledgement that it has the written consent of employees and prospective employees to access their driving license information via the Employer Notification program.

i.) maintain in its records the written consent for the time periods specified in this agreement. The SCDMV will have the right to request that the User provide to the SCDMV copies of any specific consents or categories of consent; such copies will be provided to the SCDMV by mail, facsimile, email, or other means within fifteen days of a SCDMV request.

j.) not to use, sell, assign, or otherwise impart to any person, firm, or corporation any personal information obtained from SCDMV records, including listings of individuals, for any reason.

Documentation on the Employer Notification Service is available at www.scdmvonline.com. Documentation for the SCDMV Member Services Security will be made available upon execution of this contract.

2. PERMISSIBLE USE

The User agrees that the records it receives will not be used for any purpose other than the purpose for which the permission for access was originally granted pursuant to the DPPA as provided in this agreement. User may retain copies solely to comply with retention requirements imposed by applicable state or federal law.

3. RETENTION OF RECORDS

User understands and agrees that all data received from the SCDMV pursuant to this agreement that contains personal information is and remains property of the SCDMV. Notwithstanding the termination of this agreement, with regard to any retained personal data received from the

SCDMV, the User remains subject to the obligations and requirements set forth in this agreement regarding the handling, use, audit and protection of all personal data received.

4. AUDIT AND AUDIT REIMBURSEMENT

The User acknowledges and agrees that the SCDMV, or an independent auditor selected by the SCDMV, may audit the performance of the User under this agreement, to include follow up audits if discrepancies or deficiencies are found. The degree and conduct of any such audit, and the frequency of such audits, will be at the sole discretion of the SCDMV and will focus on compliance with the terms of this Agreement. The User agrees to assume responsibility for the actual costs of all such audits and will submit payment for audit within thirty calendar days of receipt of an invoice. The User agrees to cooperate fully with the SCDMV's auditors.

5. TERMINATION

Either party may terminate this agreement upon thirty calendar days written notice to the other party unless a shorter time is agreed upon by both parties.

The SCDMV may immediately cease providing information without a hearing upon the User's breach of, or failure to fulfill, any responsibility established pursuant this agreement.

If, to its own satisfaction, the SCDMV determines that the User has either misused or knowingly allowed the misuse of any information provided to the User pursuant to this agreement, the SCDMV may, in addition to other penalties provided by law:

(a) Terminate this agreement immediately;
(b) Require the return of all files and media containing information provided by the SCDMV;
(c) Require the deletion of all electronic files containing information provided by the SCDMV; and
(d) Take any other actions that the SCDMV deems appropriate to protect the interests of the SCDMV and the citizens of the State of South Carolina.

If court orders are issued or if the laws, rules, or regulations change such that the terms of this agreement cannot be fulfilled, the agreement will be automatically and immediately terminated.

6. MODIFICATION

This agreement is subject to change and modification due to changes in the SCDMV's policies, the issuance of court orders, or changes in State and/or Federal laws, rules, and regulations. Should the SCDMV change its policies such that the terms of this agreement must be modified, the User will be notified at least thirty calendar days in advance of such changes or modifications and the User, at its option, may immediately terminate this agreement.

This agreement cannot be modified in any manner except by written amendment or agreement change order that has been executed by the parties.

7. MISCELLANEOUS

This agreement is the exclusive statement of the parties with respect to its subject matter and supersedes all prior agreements, negotiations, representations, proposals, and awards, written and oral, relating to its subject matter.

8. TECHNICAL REQUIREMENTS FOR DATA ACCESS

User agrees that these guidelines apply to any computer used to access SCDMV information.

1. Computers (workstations and servers) must be running a current and supported operating system. Your organization must have a well-defined process to ensure that operating systems are patched with the latest updates within a month of release.

2. Computers (workstations and servers) must be running a current and supported anti-virus solution. The anti-virus solution must provide real-time protection. Your organization must have a formal process to keep your anti-virus solution current and ensure that virus definition updates are applied daily.

3. Organizations must use a security monitoring solution for the devices on its network, with event logging enabled. Monitoring solutions can be at the network level or at the workstation level. A combination of the two, with third party monitoring is preferred.

4. All non-removable storage in laptops should be encrypted with at least 256 bit AES encryption.

5. All computers used to access SCDMV data should be behind a firewall.

6. Users are not authorized to distribute/copy/save/print any information accessed on SCDMV's website or through the Member Services Portal, except as otherwise provided herein.

9. NOTICE OF BREACH PROTOCOL

Security Incident and/or Data Breach: In an actual or suspected security-related incident and/or real or possible data breach that may or will impact the SCDMV's information systems or data containing personally identifiable information (PII), the User must notify the SCDMV's IT Security Administrator within twenty-four hours after initially discovering the aforementioned circumstances. The User will provide the SCDMV's IT Security Administrator with a written, detailed explanation of the incident, including any SCDMV exposure, incident mitigation, and the corrective actions taken within seventy-two hours of the initial discovery of the incident. Initial notification may be telephonic to the SCDMV's IT Security Administrator, followed by a written explanation within seventy-two hours. The description must include details specific to any PII that

was, may have been, or may yet be compromised and incident mitigation and corrective actions taken to protect PII against unauthorized access, use, or disclosure. The SCDMV reserves the right to request the offending individual(s) be removed from the SCDMV's account. For purposes of this agreement, PII has the same meaning as the definition of "personal information" and "highly restricted personal information" as found under the DPPA. The SCDMV will restore data access upon satisfactory review of a third-party attestation surrounding the facts and remediation of the security incident.

Contact Information for SCDMV's IT Security Administrator

SCDMV's IT Security Administrator
Primary Contact: Wesley Belk: 803-240-6932
Alternate Contact: Deborah Mangels: 803-766-8659
Email: isonotify@scdmv.net

10. DESTRUCTION

Except as may be reasonably necessary to prove record keeping compliance with applicable law, the User shall be responsible for destruction and disposal of SCDMV data it has received as set forth herein.

All destruction/disposal of media, digital or physical, will be in accordance with State and Federal laws, regulations, and industry best practices commensurate with the data classification. All removable media used by User in the execution of this Agreement will be properly classified in accordance with the South Carolina Department of Administration, Division of Information Security and the SCDMV policy, audited, and encrypted in accordance with industry best practices and commensurate with the classification of the data.

User shall assume all disposable and removable media used in the execution of this agreement contains restricted or confidential data, and, therefore, must treat all disposable and removable media, electronic and physical, with the protections and disposal procedures in accordance with this Agreement.

Before reuse of any media used in the execution of this Agreement, all Data will be sanitized in accordance with industry best practices to ensure data is rendered inaccessible and otherwise unrecoverable.

User will ensure all media containing the SCDMV Data is disposed of using methods that ensures the Data cannot be recovered or reconstructed.

User will periodically reassess its methods of destruction, disposal, and reuse to ensure methods used are based on current State and Federal laws and technology and industry best practices.

User will ensure all employees, representatives, and agents of User, upon termination of the Agreement, will return or destroy/dispose of all the SCDMV data in accordance with this Agreement.

Records involved in any open investigation, audit or litigation must not be destroyed/disposed until the matter has been closed.

11. GENERAL NOTIFICATION

All notices, communications, or reports required or permitted under this agreement, except as provided in Section **9**. **NOTICE OF BREACH PROTOCOL,** shall be sent by mail or transmitted electronically via email. Notice shall be deemed effective on the earlier of the following dates:

(1) Five business days after the date of mailing of the notice to the address listed in this agreement, with sufficient postage; or
(2) The date on which notice is acknowledged as received by the SCDMV or User through a written email confirmation.

The parties are required to keep contact information for notification purposes up to date at all times. Each party shall notify the other of any changes to contact information for notification purposes within thirty calendar days of any change. For purposes of notice under this agreement, except as to **9**. **NOTICE OF BREACH PROTOCOL,** the notice for the parties is as follows:

For User:

User:
Attention:
Address:

Telephone:
Email:

For SCDMV: South Carolina Department of Motor Vehicles
Attention: Procurement
Post Office Box 1498
Blythewood, South Carolina 29016
Telephone: 803-896-7858
E-mail: procurement@scdmv.net

12. USER SECURITY ADMINISTRATOR (SA) - ADMINISTRATOR ACCOUNT

The User's Security Administrator is designated as follows:

_____
Security Administrator's Name (print name)

_____
Security Administrator's User's Email

_____
Security Administrator's Phone Number

13. CONSTRUCTION

The language in all parts of this Agreement shall be, in all cases, construed according to its plain meaning and not strictly for or against either of the parties.

14. SCOPE OF AGREEMENT

The parties acknowledge that this agreement constitutes the entire agreement between User and SCDMV and that any representations or communications or between the parties that are not contained within the body of this writing, are unenforceable, non-binding and are outside of the scope of the obligations of either party.

15. SIGNATURES

As witness herein, the parties hereto have affixed their signatures and seals. This Agreement may be executed in counterparts, each of which may be enforceable as an original, but all of which together shall constitute but one agreement. Facsimile and PDF copies of this Agreement shall be treated the same as originals. The undersigned represent and warrant that he/she is an officer of the organization for which he/she has executed this agreement and that he/she has the full and complete authority to enter into this agreement on behalf of the User, thereby binding the User, its personnel, its agents, and its representatives to the certifications, terms, and conditions as stated in this agreement.

User Name: Account #

USER

_____
User Agency Name

_____
User's Authorized Representative (*signature*)

_____
User's Authorized Representative (*print name*)

_____
User's Authorized Representative's Title (*print title*)

_____
Date

SOUTH CAROLINA DEPARTMENT OF MOTOR VEHICLES

_____
Executive Director or designee (*signature*)

_____
Print Name

_____
Print Title

_____
Date