

**Attachment #1**

**GUIDELINES FOR PROJECT TO REDUCE FRAUDULENT CHECK WRITING WITH \_\_\_\_\_.**

**Each bank employee with access to OMV information shall read and sign this document. The original of this document shall be maintained by the bank in the manner provided in the bank's memorandum of understanding or as approved by the Department of Public Safety and Corrections, Office of Motor Vehicles.**

Individual personal information provided by the Department of Public Safety and Corrections, Office of Motor Vehicles (OMV), from driver's license, identification card, or vehicle records is subject to the Federal Driver Privacy Protections Act (DPPA). 18 U.S.C. §2721 et seq. In connection with this project to reduce fraudulent check writing, \_\_\_\_\_ has requested access to personal information from OMV records on driver's licenses, identification cards, or vehicle registrations/titles.

In accordance with 18 U.S.C. §2721(b)(3), OMV is providing this information to \_\_\_\_\_ solely for the purposes of this project to reduce fraudulent check writing.

\_\_\_\_\_ agrees to disclose the personal information provided by OMV only to its employees, agents, contractors, subcontractors, or other representatives who are working directly on the pilot project to reduce fraudulent check writing. Any other disclosure is prohibited.

\_\_\_\_\_ is responsible for ensuring that its employees, agents, contractors, subcontractors, or other representatives with access or control over personal information are trained and educated with regards to the requirements of the DPPA.

\_\_\_\_\_ further acknowledges its duty under the DPPA, in particular, 18 U.S.C. §2721(c), to maintain records regarding its disclosure of personal information to its employees, agents, contractors, subcontractors, or other representatives.

\_\_\_\_\_ shall use current and updated security and internal controls to protect the personal information of individuals from a breach of security. Breach of the security of the system means the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by the Contractor.

The electronic transmission of any personal information received by \_\_\_\_\_ from the Department shall be encrypted or transmitted over a secure line. Transmission of personal information via e-mail or unencrypted via the Internet is strictly prohibited.

\_\_\_\_\_ shall promptly notify OMV if personal information has been accessed through any means that defeats the Contractor's security or internal controls, which access is contrary to federal or state privacy laws, unless directed to do otherwise by a law enforcement officer investigating the unauthorized access described in this paragraph.

Personal information means information that identifies an individual, including an individual's driver license number, name, and address (but not the 5-digit zip code), but does not include information on vehicular accidents, driving violations, and driver's status.

\_\_\_\_\_ shall have each employee, agent, contractor, subcontractor, or other representative with access or control over personal information, read, sign, and date a copy of this document to acknowledge that person has received a copy of this documents and that such person is familiar with the information contained in this document and understands this document. \_\_\_\_\_ shall maintain the signed original of this document for a period of five years, and shall make the original document available to OMV upon request as required by 18 U.S.C. §2721(c). As an alternative, \_\_\_\_\_ may maintain the file in electronic format that is acceptable to OMV as long as the file is protected in a manner such that once the file is created, it can only be read.

\_\_\_\_\_  
Signature of \_\_\_\_\_ Employee      Date

\_\_\_\_\_  
Printed Name of \_\_\_\_\_ Employee