This Service Description is part of the Treasury Services Master Agreement, Global Treasury Management Services Master Agreement, or other master agreement for treasury and payment services (the "*Master Agreement*") in effect between you and BMO Bank N.A. ("*Bank*"), and is subject to all of the terms and conditions contained in the Master Agreement. Any references herein to the Master Agreement shall be deemed to include the terms of this Service Description, including any User Guide and set-up form. Any capitalized terms not defined herein shall have the same meaning as set forth in the Master Agreement. By accepting this Service Description as part of the Master Agreement, you agree to the following terms and conditions in connection therewith.

1. The Service.

Under this service (the *"Service"*), Bank will grant you access to the Real-time Payment Chek® Service with Account Owner Authentication (*"AOA"*) provided in cooperation with our third-party service provider, Early Warning Services, LLC, along with its affiliates that may be involved in providing the Service (together, *"EWS"*). The Service allows you to validate the ownership, signatories, and status of deposit accounts of third parties. The validation is performed either in real time or by batch process against cross-bank contributed account data stored in a National Shared Database maintained by EWS.

The Service is made available to you in part pursuant to an agreement between Bank and EWS. EWS maintains the National Shared Database and is responsible for validating Inquiry Data against the National Shared Database and transmitting Response Data as described herein, as well as other administrative services in connection with the Service. EWS will be a third-party beneficiary to this Service Description and the Master Agreement (insofar as it applies to the Service), entitled to the benefits and protections of their applicable terms and conditions.

Before accessing the Service, you must complete the required Service Documentation which must be accepted by Bank. You must also complete the required setup procedures. If you wish to access any of the Services which are available through Online Banking for Business (*"OLBB"*), you must also sign up for the OLBB service and complete the applicable Service Documentation and setup process and Bank must agree to provide that service to you. In order to utilize the Service in connection with initiating payments, you must also sign up for the relevant payment service and complete the applicable Service Documentation and setup procedures and we must agree to provide that service to you. .

2. Definitions.

As used in this Service Description:

(a) *"Client Account"* means an account (as defined in Regulation CC, 12 C.F.R. § 229.2(a)) held by a consumer or business with you, and may also include a savings account, a money market account, a credit account, or a brokerage account held by a consumer or a company with you if you are a Financial Services Organization or other business relationship currently existing or pending between you (if you are a Financial Services Organization) and a consumer or a company;

(b) *"FCRA"* means the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 *et. seq.*;

(c) *"Financial Services Organization"* means an entity that provides banking, insurance and/or investment products and services, and is regulated by one or more of the following entities: Office of the Comptroller of the Currency, Consumer Financial Protection Bureau (excluding non-depository covered persons), National Credit Union Association, Securities and Exchange Commission, Financial Industry Regulatory Authority (formerly NASD), Federal Reserve, Federal Deposit Insurance Corporation, Public Corporation for the Supervision and Insurance of Cooperatives in Puerto Rico (COSSEC), or state banking departments or state insurance commissioners (Department of Insurance and similarly named organizations);

(d) *"Government Agency"* means a local, state or federal government agency and its contractors;

(e) *"Inquiry"* means each request for Response Data from the National Shared Database transmitted by you to EWS directly or to Bank for forwarding to EWS, as selected by you in accordance with Section 3(b);

(f) *"Inquiry Data"* means the information contained within an Inquiry;

(g) *"National Shared Database"* means the collection of data maintained by EWS in one or more databases for use in providing the Service and other services EWS may offer from time to time;

(h) *"Participant as Processor"* means a user of the Service that provides a response that is comprised of or derived from, in whole or in part, Response Data, to its own customers that are the end users of the Response Data;

(i) *"Response Data"* means information from the National Shared Database transmitted by EWS in response to an Inquiry to you directly or to Bank for forwarding to you, as selected by you in accordance with Section 3(b); and

(j) *"Technical Integrator"* means any third party designated by you or, if you are a Participant as Processor, your customer (end user), that has physical, logical or network access to Inquiry Data, Response Data, and any other EWS data transmitted between any of these parties or the systems that house any such data. For the avoidance of doubt, a third party shall be considered a Technical Integrator if it receives and transmits a response comprised in whole, or in part, of Response Data.

3. Description and Terms of Service.

(a) Grant of Access Rights. Subject to the terms of this Service Description, Bank grants to you a non-exclusive, revocable, non-transferable, and limited right to access and use the Service in accordance with the terms of this Service Description and for your internal business purposes only. You may not sell, resell, sublicense, or otherwise transfer or provide, directly or indirectly, the Service, or any portion of thereof (including Response Data and other content), to any third party except as expressly permitted in this Service Description. You acknowledge that the Real-time Payment Chek® Service with AOA and the National Shared Database are proprietary to EWS and that you receive no copyright, intellectual property rights, or other rights (other than those described in this Service Description) in or to any of the foregoing. EWS retains all rights, title and interests in and to the Real-time Payment Chek® Service with AOA and the National Shared Database, including any enhancements thereto, whether conceived by you, EWS, or otherwise. You will protect and not violate those proprietary rights and honor and comply with Bank's reasonable requests to protect Bank's and EWS's contractual, statutory, and common law rights in the Real-time Payment Chek® Service with AOA and the National Shared Database. If you become aware of any violation of Bank's or EWS's proprietary rights, you will promptly notify Bank in writing. You agree that you shall not attempt to reverse engineer, recreate, or otherwise copy the Service and shall not assist any other person, directly or indirectly, in any attempt to reverse engineer, recreate, or otherwise copy the Service.

(b) Access Methods. You may access the Service (i) through a direct connection with EWS, (ii) by transmitting Inquiries and receiving Response Data through your direct connection with Bank or through Bank's OLBB service if you have subscribed for OLBB, or (iii) by such other means as may be made available by Bank from time to time and expressly approved by Bank in writing. If you elect to access the Service through a direct connection with EWS, you must execute and deliver to EWS a connectivity agreement that Bank will separately provide to you (the *"Connectivity Agreement"*).

You must use the passwords and other Security Procedures that Bank may issue to you or otherwise establish for you from time to time to access or otherwise in connection with the Service. You are solely responsible for ensuring that the Security Procedures are known to and used only by those authorized users within your organization (*"Authorized Users"*) as identified in the Service Documentation. In Bank's discretion, Bank may deny access to the Service to any user.

You will notify Bank immediately if you become aware of any unauthorized access to or use of the Service, or if any Security Procedures have been lost, stolen, or compromised. You will cooperate with Bank in any investigation and agree to take corrective measures to protect your account from further unauthorized use or fraudulent activity. You will provide to Bank and keep current all information Bank reasonably requires from time to time with respect to each Authorized User and will notify Bank immediately if an Authorized User ceases to be associated with your organization or is no longer authorized to access the Service on your behalf, or if for any other reason you would like to modify or remove an Authorized User's access to the Service. In Bank's sole discretion, Bank may terminate, revoke, suspend, modify, or change any or all Security Procedures at any time with or without prior notice.

(c) Inquiries and Response Data. You may initiate Inquiries and receive Response Data pursuant to the terms and conditions of this Service Description. The required technical layout requirements for each type of Inquiry Data, as well as the potential types of Response Data and their technical layout requirements, are set forth in the following reference: *Real-time Payment Chek Service with Account Owner Authentication Inquiry Technical Requirements for Payment Processors*.

You acknowledge and agree that Response Data is time-sensitive and only intended to be used in connection with the specific Inquiry for which it was requested. You agree that you will not merge, aggregate, or compile Response Data into any other database for use in connection with future Inquiries.

(d) Authorized Uses of Response Data. You may use the Service and Response Data solely for the purposes set forth in Exhibit B.

(e) Representations and Warranties. In order to induce Bank and EWS to provide the Service to you, you represent and warrant to Bank and EWS each time you use the Service that (i) you are either (x) a Government Agency, or (y) a business entity that is not a Financial Services Organization, unless approved in writing by Bank, and (ii) you are either (x) the end user of the Response Data, including any response that is comprised of or derived from, in whole or in part, Response Data, received by you in response to your Inquiries, or (y) a Participant as Processor acting in compliance with Section 5. You agree to provide Bank, promptly upon request, a written certification that the representations and warranties in this paragraph are true and correct.

(f) Market and Business Limitations. Bank and EWS may from time to time limit or prohibit the markets and/or types of businesses that are eligible to receive Response Data. Bank may require you to provide information and/or documentation to allow Bank to verify, in a manner acceptable to Bank, that Bank and EWS are providing Response Data only to those markets and/or types of business that are eligible to receive such responses.

(g) Technical Integrators. If you elect to use a Technical Integrator for the transmitting of Participant Data, the transmitting of Inquiries/Inquiry Data, and/or the receiving of Response Data, you agree to comply with the requirements of Exhibit C. If you are a Participant as Processor and your customer (end user) elects to use a Technical Integrator for the transmitting of Participant Data, the transmitting of Inquiries/Inquiry Data, and/or the receiving of Response Data, you shall ensure that such customer complies with the requirements of Exhibit C.

(g) Compliance with Law; FCRA Obligations. You agree to comply with all Applicable Laws in connection with your use of the Service, including, without limitation, all applicable provisions of the FCRA. You acknowledge receipt of the notices attached hereto as Exhibit D, which describe certain obligations of (i) furnishers of information to consumer reporting agencies, and (ii) users of consumer reports, and, to the extent applicable, you agree to comply with such obligations. If you use Response Data to take "adverse action" against a "consumer" (each such term as defined in Section 603 of the FCRA) about whom the Response Data relates, you agree to refer such consumer to EWS for handling disputes concerning the completeness or accuracy of any item of information contained within the Response Data.

4. Contribution Requirements.

If you are a Financial Services Organization with 250,000 or more Client Accounts, then, as a condition of using the service, you shall be required to contribute data to the National Shared Database. Please contact your Bank representative for more information about data contribution requirements. Financial Services Organizations that are insurance companies (defined as institutions that provide insurance policies to protect individuals and businesses against the risk of financial losses in return for regular payments of premiums) or investment services companies and do not offer transaction-able accounts (i.e. ACH, check payments, etc.), are not subject to the contribution requirements of this Section 4.

5. Participants as Processors.

This Section applies to you if you are a Participant as Processor.

(a) You will assign each of your customers that receives any response that is comprised, in whole or in part, of Response Data a unique identification number (*"Client ID"*). Additionally, if Inquiries are transmitted for multiple divisions or affiliates of a customer, you will assign each such division and/or affiliate a unique Client ID in the Inquiry file in all Inquiries transmitted for such customer. You shall not use any Client ID in any Inquiry that is made for a customer, any of its divisions or its affiliates, other than the customer, applicable division or affiliate for which such Client ID is assigned. Bank will define how the various Client ID fields within the Inquiry file are required to be populated during the implementation phase.

(b) You will transmit to your customers only a translated decision such as an "accept" or "decline" decision and shall not transmit to your customers Response Data unchanged. You shall not permit any customer that receives a response that is comprised of or derived from, in whole or in part, Response Data, to sell, resell, sublicense, or otherwise transfer or provide, directly or indirectly, the Service, or any portion thereof (including Response Data and other content), to any third party, unless approved in writing by Bank.

(c) Bank may suspend or terminate the provision of Response Data to you upon notice to you if you do not comply with the requirements of this Section or if Bank is unable to verify your compliance, to Bank's reasonable satisfaction.

(d) If you receive notice, from any source, that (i) a customer that receives any response comprised of or derived from, in whole or in part, Response Data, (ii) any individual or entity that holds a controlling interest in such customer, (iii) any member of the customer's board of directors or equivalent governing body, (iv) any officer or manager of such customer, or (v) any other employee that has access to Response Data or has decision-making authority on how the Service is used or marketed (each of the foregoing, a *"Regulated Party"*), is the subject of an investigation or other action by any Federal, state or local governmental, administrative or regulatory body, you will immediately notify Bank of such investigation or other action. Bank, in its sole discretion, may require that you cease providing responses comprised in whole or in part of Response Data to that customer. Not more than five (5) days following your receipt of Bank's notification to cease providing such responses to the customer, you will provide Bank with written certification that you (i) have ceased providing, (ii) do not currently provide, and (iii) will not provide in the future (unless approved in writing by Bank), responses comprised, in whole or in part, of Response Data to the customer that is subject to, or is controlled by a Regulated Party that is subject to, the investigation or action.

(e) You will establish and maintain procedures for assessing your customers that receive any response that is comprised of or derived from, in whole or in part, Response Data. Such procedures shall meet or exceed the Minimum Requirements for Customer Vetting attached hereto as Exhibit A, which may be modified by Bank upon notice to you (the *"Vetting Requirements"*). Bank shall have the right, once per calendar year, to review your vetting procedures and evidence of such customer assessments completed by you. In addition to the foregoing annual audit rights, you agree that if Bank reasonably believes that you are not complying with the Vetting Requirements, Bank shall have the right to inspect your records and procedures related to your obligations under this Section during normal working hours, and in a manner as to minimize interference with your normal business activities.

(f) You agree to provide Bank, no later than the fifth (5th) day of each calendar quarter, with (a) a list of all of your customers that receive any response that is comprised, in whole or in part, of Response Data and (b) a written certification that such customers are the end users of the Response Data, including any response that is comprised of or derived from, in whole or in part, Response Data, they receive. The list required by this Section shall include each customer's name, physical business address, merchant identification number, customer type classification (i.e. point of sale, payment acceptance, check casher, etc.), and the date that that party was implemented to receive any response that is comprised, in whole or in part, of Response Data.

(g) You agree that Bank shall have the right to approve any of your customers that receives a response that is comprised of or derived from, in whole or in part, Response Data.

6. Confidentiality.

(a) You agree (i) to restrict access to the Response Data to those of your employees, contractors, subcontractors, attorneys, auditors, and accountants who have a legitimate business need to know such information, (ii) to take appropriate action by separate agreement having terms no less restrictive than the terms of this Section with those employees, contractors, subcontractors, attorneys, auditors, and accountants having access to the Response Data to fulfill your obligations under this Section, (iii) not to use or disclose any Response Data for any purpose other than the permitted purpose for which such information was provided, and (iii) to use at least the same degree of care to avoid unauthorized disclosure or use of Response Data as you use to protect your own confidential information, but no less than a reasonable degree of care. You agree to be responsible for any breach of this Section by any of your employees, contractors, subcontractors, attorneys, auditors, and accountants.

(b) To the extent that any Response Data is "nonpublic personal information" about "consumers" or "customers" as such terms are defined in Title V of the Gramm-Leach-Bliley Act (*"GLBA"*), 15 U.S.C. § 6802, and in regulations issued thereunder (collectively, *"Consumer Data"*), then in addition to your obligations under Section 6(a), you agree that you will not disclose or use such Consumer Data in any manner prohibited by the GLBA or the regulations issued thereunder. You further agree to maintain appropriate measures designed to meet the objectives of the applicable guidelines establishing information security standards as adopted by any federal regulatory agencies having jurisdiction over your affairs. These measures include appropriate disposal of Consumer Data, as required, and taking appropriate actions to address incidents of unauthorized access to sensitive Consumer Data, including notification to Bank as soon as possible of any such incident.

7. Information Security Requirements for Direct Connections.

This Section applies to you if you access the Service through a direct connection with EWS or Bank. This Section does not apply to you if you only access the Service through OLBB.

(a) You agree to maintain a written information security program that contains administrative, technical and physical safeguards designed to: (i) ensure the security and confidentiality of Response Data, (ii) protect against any anticipated threats or hazards to the security or integrity of Response Data, (iii) protect against unauthorized access to or use of Response Data that could result in substantial harm or inconvenience to you or any customer or consumer, (iv) limit access, use and disclosure of Response Data as expressly permitted by this Service Description, (v) ensure the proper disposal of Response Data, (vi) ensure the encryption of Response Data at rest using a current industry acceptable encryption method (e.g., AES-256 or stronger encryption), and (vii) comply with applicable law. Your information security program must be designed to: (1) meet the objectives of the Interagency Guidelines Establishing Information Security Standards promulgated by the federal banking agencies as amended from time to time, and (2) include control objectives that meet applicable industry standards such as ISO 27002, FFIEC, OCC, PCI, or NIST. You agree to promptly notify Bank of any modification to your information security program that causes the security program to fail to comply in all material respects with this Section. You represent and warrant that your information security program is reasonably designed to meet the foregoing requirements.

(b) Bank and EWS shall have the right, during normal business hours, upon reasonable advance notice, and not more than once per calendar year, to conduct an on-site audit of your information security program and related policies, controls, processes and procedures. In addition, you agree to complete a Shared Assessment Significant Information Gathering (SIG) Questionnaire or provide to Bank and EWS, upon request, a copy of your most recent third party data processing audit or review (e.g., SOC2-Type II, ISAE 3402, SSAE 16 or equivalent based upon American Institute of Certified Public Accountants (AICPA) standards, Acceptable Use Procedures (AUP), etc.) as conducted by your external auditors related to the Service or the ACH Origination/ACH Third Party Servicer/Sender service.

(c) Bank and EWS shall have the right, during normal business hours, and not more than once per calendar year, upon reasonable advance notice, to audit your relevant processes and procedures to verify your compliance with the terms of this Service Description.

(d) In the event of a breach in security resulting in actual or suspected loss of or unauthorized access to Response Data, you shall: (i) immediately notify Bank by calling Bank's Information Protection Centre as follows: (1) Monday to Friday, 8:00 a.m. to 4:00 p.m. Eastern time, by calling 416-502-5959, and (2) after hours, by calling 1-866-265-2182, Option 1, and requesting that the Information Protection Centre Security Incident Response team be paged; (ii) immediately notify EWS by calling (877) 275-7774, Option 4; (iii) conduct a forensic examination to determine to what extent Response Data was compromised; (iv) provide to Bank and EWS, in writing, details concerning the breach, including: (1) nature and impact of the breach, (2) assessment of immediate risk due to the breach, (3) corrective actions already taken, and (4) corrective actions to be taken; (v) cooperate with Bank, EWS, any other affected parties, regulators, or law enforcement to assist in regaining possession of the Response Data and in preventing its further unauthorized use and to notify affected consumers if required by applicable law; and (vi) take measures to restore and enhance your security policies and procedures to avoid further breaches.

(e) You shall not knowingly permit any of your directors, officers, employees, contractors, subcontractors, attorneys, auditors, and accountants to access the Service if the person has been (i) convicted of a crime in connection with a dishonest act, breach of trust, or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, as described in Section 19 of the Federal Deposit Insurance Act, 12 U.S.C. § 1829(a), or (ii) convicted of a felony.

8. EWS Information Security.

(a) Upon request by you, and subject to your execution of a confidentiality agreement acceptable to EWS, Bank will make available to you a copy of EWS's most recent Annual Risk Report, as well as any updated EWS Annual Risk Report.

(b) If, in addition to the information provided as described in Section 8(a) above, you require to conduct an on-site audit of EWS's information security program outside of EWS's regularly scheduled consolidated on-site audit periods (which are free to you), then a daily fee shall be assessed to you by EWS for the on-site audit. Any on-site audits (i.e. outside of the regularly scheduled consolidated on-site audit periods) shall not begin until the daily fee for each, as applicable, has been agreed upon between you and EWS. Fees related to these on-site audits will be billed to you separately from fees for the Service. However, any on-site audit that is triggered by a regulatory requirement or a court order will not result in a daily fee as set forth herein. Please contact your Bank representative for more information about on-site audits of EWS's information security program.

(c) If, in addition to the information provided as described in Section 8(a) above, you require that EWS complete a questionnaire regarding EWS's information security program, then a fee shall be assessed to you by EWS for the questionnaire. Any completion of a questionnaire in this instance shall not begin until the fee for each, if applicable, has been agreed upon between you and EWS. Fees related to the completion of questionnaires by EWS will be billed to you separately from fees for the Service. Please contact your Bank representative for more information about questionnaires regarding EWS's information security program.

9. Authorized Use of Data by EWS.

You authorize EWS to use Inquiry Data and Participant Data for the purposes of: (a) preparing statistical reports and conducting data analytics, parsing routines, data modeling, and other analyses to test and evaluate EWS's services; (b) developing and providing new services or enhancements to existing services; and (c) developing and providing services to third parties engaged in the business of offering identity theft protection services to consumers, provided that no personally identifiable information shall be returned to any such third parties. The reports and results of the analyses described in clause (a) may be provided to EWS's other inquirers and contributors, provided that such reports and analyses do not identify specific Inquiry Data or Participant Data with respect to any inquirer or contributor.

10. Limitation of Liability.

(a) NEITHER BANK NOR ANY OF ITS THIRD PARTY PROVIDERS MAKES ANY WARRANTY, EXPRESS OR IMPLIED, CONCERNING THE SERVICE. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE SERVICE IS PROVIDED ON AN "AS IS" BASIS AT YOUR SOLE RISK. BANK AND ITS THIRD PARTY PROVIDERS EXPRESSLY DISCLAIM ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, INCLUDING ANY WARRANTY FOR THE USE OR THE RESULTS OF THE USE OF THE SERVICE WITH RESPECT TO ITS CORRECTNESS, QUALITY, ACCURACY, COMPLETENESS, RELIABILITY, PERFORMANCE, TIMELINESS, OR CONTINUED AVAILABILITY. NEITHER BANK NOR ANY OF ITS THIRD PARTY PROVIDERS SHALL HAVE ANY RESPONSIBILITY TO MAINTAIN THE DATA AND SERVICES MADE AVAILABLE THROUGH THE SERVICE OR TO SUPPLY ANY CORRECTIONS, UPDATES, OR RELEASES IN CONNECTION THEREWITH. AVAILABILITY OF DATA AND SERVICES ARE SUBJECT TO CHANGE WITHOUT NOTICE.

(b) YOU ACKNOWLEDGE THAT ELECTRONIC ACCESS TO SYSTEMS THROUGH THE INTERNET OR OTHER NETWORKS, WHETHER PUBLIC OR PRIVATE, MAY NOT BE SECURE. NEITHER BANK NOR ANY OF ITS THIRD PARTY PROVIDERS MAKES ANY WARRANTY WHATSOEVER TO YOU, EXPRESS OR IMPLIED, REGARDING THE SECURITY OF THE SERVICE, INCLUDING WITH RESPECT TO THE ABILITY OF UNAUTHORIZED PERSONS TO INTERCEPT OR ACCESS INFORMATION TRANSMITTED BY YOU THROUGH THE SERVICE, AND BANK AND ITS THIRD PARTY PROVIDERS DISCLAIMS ALL LIABILITY FOR ANY SECURITY BREACH THAT DOES NOT RESULT FROM SUCH PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

(c) Neither Bank nor any of its third party providers shall have any liability, contingent or otherwise, to you or to third parties, or any responsibility whatsoever, for the failure of any connection or communication service to provide or maintain your access to the Service, or for any interruption or disruption of such access or any erroneous communication among Bank and you, regardless of whether the connection or communication service is provided by Bank or a third party service provider. Neither Bank nor any of its third party providers shall have any liability, contingent or otherwise, to you or to third parties, for the correctness, quality, accuracy, timeliness, reliability, performance, continued availability, completeness or delays, omissions, or interruptions in the delivery of the data and services available through the Service or for any other aspect of the performance of the Service or for any failure or delay in the execution of any transactions through the Service. Bank will have no responsibility to inform you of any difficulties experienced by Bank or third parties with respect to the use of the Services or to take any action in connection therewith.

(d) In addition to any other limitations on liability contained in this Service Description, the Master Agreement, or any other agreement between you and Bank, to the extent permitted by applicable law, Bank's cumulative liability to you for all loss or damage arising from or relating to this Service Description or the Service, regardless of the form of action, is limited to the amount of fees paid by you for the Service during the six months immediately preceding the month in which the loss or damage was incurred.

(e) The provisions of this Section shall survive termination of this Service Description or the Master Agreement.

11. Suspension; Termination.

Bank may suspend the Service upon notice to you if you do not comply with the requirements of this Service Description or if Bank is unable to verify your compliance with the requirements of this Service Description to Bank's reasonable satisfaction. Bank may suspend or terminate the Service upon notice to you if it determines that you conduct business of the type and/or within a market that is ineligible to use the Service as described in Section 3(f) above. Bank may also suspend or terminate the Service upon notice to you if Bank's agreement with EWS in connection with providing the Service is terminated or if EWS otherwise ceases to support the Service for any reason.

In addition to Bank's termination rights as set forth in the Master Agreement or elsewhere in this Service Description, Bank shall have the right to terminate the provision of Response Data upon five (5) days written notice to you if (a) any Response Data provided to you is used or disclosed by you in violation of any applicable law, this Service Description, or the Connectivity Agreement, or (b) you experience any incident that materially jeopardizes the security of any Response Data in your possession, or (c) you, any individual or entity that holds a controlling interest in you, any member of your board of directors or equivalent governing body, any of your officers or managers, or any other employee of yours that has access to Response Data or has decision-making authority on how the Service is used is the subject of an investigation or other action by any Federal, state or local governmental, administrative or regulatory body.

If and as requested by you upon termination of the Service or the Master Agreement, on a date mutually agreed by the parties, EWS and Bank shall meet with you to prepare and implement a plan for the secure deletion of all Participant Data. To the extent that Participant Data cannot be so deleted due to technical, regulatory, or other reasons reasonably acceptable to you, EWS shall ensure, for so long as any Participant Data remains under EWS's control, the continued protection of such Participant Data, in compliance with the confidentiality and security requirements of this Service Description.

12. Miscellaneous.

Any telephone conversations relating to the Service may be recorded at Bank's option to assure accuracy.

THIS SERVICE DESCRIPTION HAS BEEN EXECUTED AS PROVIDED IN THE SCHEDULE OF SERVICES FORMING A PART OF THE MASTER AGREEMENT.

EXHIBIT A TO ACCOUNT VALIDATION SERVICE DESCRIPTION

MINIMUM VETTING STANDARDS FOR CUSTOMERS OF PARTICIPANTS AS PROCESSORS

All customers of a Participant as Processor (where applicable) that receive a response to an inquiry where such response is comprised of or derived from, in whole or in part, Response Data must be vetted by Participant as Processor, at a minimum, to meet the requirements herein and in accordance with the procedures outlined below. For the purposes of these vetting requirements, customer includes the parent company, affiliates, and any DBA entity.

Participant as Processor must maintain:

1. Written procedures for customer vetting that meet the minimum requirements outlined in this Exhibit B under the section below titled "Minimum Vetting Requirements".
2. Such written procedures must include a process for all of the following:
    a. Completing each of the minimum requirements;
    b. Ensuring customers are not implemented to receive any response to an inquiry that is comprised of or derived from, in whole or in part, of Response Data prior to completion and clearance of the vetting process;
    c. Timely review of all existing customers;
    d. Listing and/or documenting the vetting history for each customer including dates and findings;
    e. Escalation of any negative information found or any information that cannot be verified;
        i. Must include a review by CEO or equivalent C-level employee of the Participant as Processor's team and documentation of the results.
        ii. Any approval of customer following review under 2.e.i. must include a detailed justification.
    f. Storage and review of hard copies and/or electronic copies of all evidence to support the vetting process for each requirement; and
    g. Providing required information and/or documentation to Bank as part of an audit or review to support Participant as Processor's vetting process.

New Customers:

Each new customer must be vetted and pass each of the vetting requirements prior to the customer receiving any response to an inquiry that is comprised of or derived from, in whole or in part, of Response Data and must be vetted annually thereafter.

Existing Customers:

Each existing customer as of the date of the agreement to receive Response Data, receiving any response to an inquiry that is comprised of or derived from, in whole or in part, Response Data must be vetted within twelve (12) months of execution of the agreement, and annually thereafter, not to exceed twelve (12) months since the last vetting of the customer.

Minimum Vetting Requirements:

1. Have a complete and documented understanding of the customer's business model and transaction process flow.
2. Confirm customer has: a) a legitimate business need for a response to an inquiry where such response is comprised of or derived from, in whole or in part, Response Data; and b) permissible

purpose for procurement of a consumer report in accordance with Section 604 of the Fair Credit Reporting Act (FCRA).

3. Verify that the type of business, products and/or services offered, and contact information that the customer provided on the application or questionnaire coincides with information on the customer website and is verified through other public resources.
4. Verify whether the address provided is a commercial or residential building by performing an onsite visit or appropriate Internet searches.
5. Verify the address and telephone number provided on the application is accurate by utilizing Internet searches such as Google, telephone white pages, Hoovers, Reference USA, etc., or request supporting documentation such as a copy of a current lease and/or telephone bill in the customer's name.
6. Verify the customer is active and in good standing in its state of incorporation or state of licensing by searching the state's website (e.g., Secretary of State or State Corporation Division) or obtain a certificate of good standing.
7. Verify whether the customer is the subject of a FTC or CFPB action or case by searching the FTC and CFPB websites for the business name and the names of all owners, principals, officers and directors.
8. Conduct an OFAC search for the business name and the names of all owners, principals, officers and directors.
9. Conduct a Better Business Bureau search for the business name.
10. Conduct Internet searches such as a Google search for the business name and the names of all owners, principals, officers and directors for any negative information.
11. Conduct a search of the State Attorney General's website in the customer's state of incorporation and state(s) of licensing to verify whether the business and/or any owner, principal, officer or director is subject to state action or cases.
12. Document and implement a process for handling items that cannot be verified or validated or where negative information is found, including without limitation the escalation procedures described in this Exhibit B.
13. Maintain a customer specific checklist (signed and dated) indicating each of the verification steps were completed, document all findings and keep copies of all associated back up documentation.

Note: Non-U.S. customers must go through a similar vetting process to meet the minimum vetting requirements and must be verified with the appropriate agencies of the country in which the company is doing business. Participant as Processor is responsible for compliance with any privacy laws, export laws and any other applicable laws and regulations relating to the transmission of data from and/or to such countries. Participant as Processor is further responsible for ensuring that its employees, agents, contractors, customers, and any other individuals or entities it exposes to responses comprised of or derived from, in whole or in part, Response Data are not on any U.S. Restricted Party Lists[1] and not from U.S. sanctioned destinations[2].

[1] "U.S. Restricted Party Lists" include Denied Persons Lists, the Unverified List, the Entity List, the Specially Designated Nationals List, the Debarred List, and the Nonproliferation Sanctions administered by the U.S. Department of Commerce, U.S. Department of Treasury, and U.S. Department of State.

[2] "U.S. sanctioned destinations" means entities and individuals who are incorporated in or nationals of countries upon which the U.S. Department of Commerce and the U.S. Department of Treasury have placed trade restrictions.

EXHIBIT B TO ACCOUNT VALIDATION SERVICE DESCRIPTION

PERMITTED USES

Defined Terms:

As used in this Exhibit C:

(a) *"Account Status Data"* means information relating to the status of an account with a Contributor in the form of a code;

(b) *"Contributor"* means an entity that transmits certain specific data elements to the National Shared Database;

(c) *"Item"* means either: (a) a physical check; (b) an image replacement document (IRD); (c) MICR line information; (d) an automated clearinghouse entry; or (e) an item as defined in the Uniform Commercial Code;

(d) *"Item Level Data"* means information about an account with a Contributor relating to Return Item Data and/or Stop Pay Data;

(e) *"Non-Participant Data"* means information about a Contributor's experience with an account, other than an account with the Contributor, consisting of Transit Data and Return Item Data;

(f) *"Participant Data"* means the prescribed data (as described in Exhibit A) contributed to the National Shared Database by you in accordance with Section 4 as a condition of using the Service;

(g) *"Response Data"* means information from the National Shared Database transmitted by EWS in response to an Inquiry to you directly or to Bank for forwarding to you, as selected by you in accordance with Section 3(b);

(h) *"Scored Account Data"* means information relating to an account, based upon Non-Participant Data, in the form of a code;

(i) *"Stop Pay Data"* means information about an account with a Contributor relating to stop pay instructions on an Item or range of Items associated with the account; and

(j) *"Transit Data"* means information identifying an Item by routing and account number relating to an account that is maintained by a depository Financial Services Organization.

You may use the Service and Response Data solely for the following purposes:

(1) For Inquiries based upon Account Status Data, Item Level Data, or Scored Account Data:

(A) to validate the existence of an account and the associated Account Status Data, Item Level Data, or Scored Account Data in determining whether to accept or decline an Item as payment for goods or services;

(B) as a factor in verifying, authorizing or guaranteeing a payment;

(C) to cash an Item or provide cash back from a deposit or payment;

(D) to decide whether to forward an Item for collection or represent it electronically; and

(E) to determine whether to allow an account or application to be enrolled for use in connection with future transactions by validating that the account exists and/or is in good standing.

(2) For Inquiries based upon Account Owner Elements Data:

(A) to determine whether to accept or decline an Item as payment for goods or services by validating that the consumer presenting such Item is an authorized accountholder, user, or signatory of the account on which the Item is drawn;

(B) to determine whether to accept or decline an Item as payment for goods or services by validating that the company name associated with such Item is the company name of the account on which such Item is drawn;

(C) to determine whether to accept or decline an Item as funding for an account by validating that the consumer is an authorized accountholder, user, or signatory of the account used or to be used in connection with the funding;

(D) to determine whether to transfer funds by validating that the consumer is an authorized accountholder, user, or signatory of the account used or to be used in connection with the transfer of funds; and

(E) to determine whether to allow an account to be enrolled for use in the connection with future transactions by validating that: (i) the consumer is an authorized accountholder, user, or signatory of the account; or (ii) the company name is associated with the account.

If you are a Financial Services Organization, the following are additional authorized uses of Response Data:

(1) For Inquiries based upon Account Status Data, Item Level Data, or Scored Account Data:

(A) to determine whether to accept or decline an Item for payment of a credit card, line of credit or loan (including personal and small business loans and lines of credit, auto loans, home mortgages, home equity loans and lines of credit and student loans);

(B) to delay or restrict the open to buy decision;

(C) to validate the existence of a recipient account of an outbound payment transaction and the associated Account Status Data, Item Level Data, or Scored Account Data in determining whether to transfer funds to such recipient account;

(D) to determine, as part of a fraud investigation resulting from a consumer filing an unauthorized transaction claim, whether the account exists and/or is in good standing; and

(E) if you determine that further investigation is necessary to mitigate risk based upon any of the following Response Data: Closed for Cause, Closed for Cause/Purged; Closed; Closed/Purged; Pending Closed; Post No Checks; Post No Debits; Enhances OD X/Y; Return Account; or Stop Payment, you may also use Response Data for the following purposes:

(i) as a factor in determining whether to close an existing account for a consumer or company;

(ii) as a factor in determining whether to monitor an existing account for a consumer or company; and

(iii) as a factor in determining whether to restrict or change existing account privileges for a consumer or company (including, but not limited to: (a) reducing the credit line for the account; (b) restricting account access; and/or (c) modifying account debit/withdrawal limits).

(2) For Inquiries based upon Account Owner Elements Data:

(A) to determine, as part of a fraud investigation resulting from a consumer filing an unauthorized transaction claim, whether the consumer is an authorized accountholder, user, or signatory of an account used in connection with the transfer of funds; and

(B) to determine whether to process a check order by validating that: (a) the consumer is an authorize accountholder, user or signatory of the account; or (b) the company name is associated with the account; and (c) the address is associated with the account.

If you are a Government Agency, Response Data may be used only as follows; provided, however, you may not refuse or decline a consumer or a company transaction or request based solely on such Response Data:

(1) For Inquiries based upon Account Status Data, Item Level Data, or Scored Account Data:

(A) to determine if information provided by an individual or a company meets the National Institute of Standards and Technology (NIST) Level 2 and/or Level 3 identification and authentication requirements;

(B) to validate the existence of an account and the associated Account Status Data, Item Level Data, or Scored Account Data in determining whether to accept or decline an Item as payment for goods or services; and

(C) to determine whether to allow an account or application to be enrolled for use in connection with future transactions by validating that the account exists and/or is in good standing.

(2) For Inquiries based upon Account Owner Elements Data:

(A) to direct requests for account verifications to Financial Services Organizations;

(B) to determine if information provided by an individual or a company meets the NIST Level 2 and/or Level 3 identification and authentication requirements;

(C) to determine whether to transfer funds by validating that the consumer is an authorized accountholder, user, or signatory of the account used or to be used in connection with the transfer of funds; and

(D) To determine whether to allow an account to be enrolled for use in connection with future transactions by validating that: (a) the consumer is an authorized accountholder, used or signatory of the account; or (b) the company name is associated with the account.

EXHIBIT C TO ACCOUNT VALIDATION SERVICE DESCRIPTION

TECHNICAL INTEGRATOR REQUIREMENTS

1. *"TI Customers"* means, as applicable, and for purposes of the requirements of this Exhibit C, you or, if you are a Participant as Processor, your customer, in each case that elects to use a Technical Integrator for the transmitting of Participant Data, the transmitting of Inquiry/Inquiry Data, and the receiving of Response Data in response to an Inquiry.
2. TI Customers shall enter into a written agreement with their Technical Integrator that satisfy the requirements of this Exhibit C.
3. TI Customers shall perform, annually, due diligence and review of Technical Integrator's information security related documentation, conduct a risk assessment of its information security related controls, identify findings and weaknesses in such controls, and document a remediation plan, as necessary.
4. Upon a reasonable suspicion of Technical Integrator's non-compliance with the requirements as set forth in this Exhibit C or applicable law, Bank and EWS will have the right to audit Technical Integrator, which may be performed jointly with the TI Customer.
5. At Bank's request, TI Customer will provide its agreement with Technical Integrator (redacted as necessary) to Bank for Bank or EWS's review to ensure compliance with the requirements of this Exhibit C.
6. TI Customers shall be responsible for the Technical Integrator's acts and omissions in connection with the requirements of 12(a), (b) and (c) below.
7. TI Customers acknowledge and agree that neither Bank nor EWS shall be liable for any errors in the transmission of Inquiry and Response Data and/or the failure to transmit such Inquiry and or Response Data by Technical Integrator.
8. If a TI Customer has an existing agreement with its Technical Integrator that does not satisfy the requirements of this Exhibit C, then TI Customer shall amend its agreement, as appropriate, with the Technical Integrator prior to the use of that Technical Integrator for the transmission of Inquiry or Response Data.
9. TI Customers will notify Bank in writing of any termination, replacement, or other change to its designated Technical Integrator as soon as reasonably practicable.
10. TI Customer acknowledge and agree that EWS currently requires its own agreement with Technical Integrators. Furthermore, TI Customer acknowledges and agrees that the Technical Integrator will be subject to Early Warning's vetting and risk assessment. TI Customer acknowledges that if in the future EWS does not require its own agreement with that Technical Integrator, EWS still reserves the right, in its absolute discretion, to later require an agreement between EWS and the Technical Integrator, and TI Customer shall cooperate with EWS to facilitate such an agreement.
11. TI Customer acknowledges that the requirements set forth in Section 12 below may be modified from time to time by Bank or EWS to address regulatory guidance and/or information security requirements.
12. TI Customer shall ensure that all of the provisions set forth below are placed within the agreement with its Technical Integrator:

    (a) Technical Integrator shall maintain an information security program that meets the requirements of Section 7(a) of the Service Description; (b) Technical Integrator shall be subject to confidentiality provisions no less restrictive than the confidentiality provisions of the Service Description; (c) Technical Integrator shall not transmit Response Data received in response to an Inquiry to any party other than in response to an Inquiry initiated by that specific TI Customer, and (d) Technical Integrator shall not merge, aggregate, or compile Response Data into any other database for use in connection with future Inquiries.

EXHIBIT D TO ACCOUNT VALIDATION SERVICE DESCRIPTION

FCRA NOTICES

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 the CFPB's website. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

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

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

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

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

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

B. Users Must Provide Certifications

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

C. Users Must Notify Consumers When Adverse Actions Are Taken

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

1. Adverse Actions Based on Information Obtained From a CRA

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

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

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

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

3. Adverse Actions Based on Information Obtained From Affiliates

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

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

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of the 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 address in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are available at http://www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records

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

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

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

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

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

A. Employment Other Than in the Trucking Industry

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

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

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

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

B. Employment in the Trucking Industry

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

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

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

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

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

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

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes - or in connection with a credit transaction (except as provided in federal regulations) - the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF ''PRESCREENED'' LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(l), 604(c), 604(e), and 615(d). This practice is known as ''prescreening'' and typically involves obtaining from a CRA a list of consumers who meet certain pre-established criteria. If any person intends to use

prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

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

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

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

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:

  (1) the identity of all end-users;

  (2) certifications from all users of each purpose for which reports will be used; and

  (3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

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

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

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

Section 602	15 U.S.C. 1681
Section 603	15 U.S.C. 1681a
Section 604	15 U.S.C. 1681b
Section 605	15 U.S.C. 1681c
Section 605A	15 U.S.C. 1681cA
Section 605B	15 U.S.C. 1681cB
Section 606	15 U.S.C. 1681d
Section 607	15 U.S.C. 1681e
Section 608	15 U.S.C. 1681f
Section 609	15 U.S.C. 1681g
Section 610	15 U.S.C. 1681h
Section 611	15 U.S.C. 1681i
Section 6l2	15 U.S.C. 1681j
Section 613	15 U.S.C. 1681k
Section 614	15 U.S.C. 1681/
Section 615	15 U.S.C. 1681m
Section 616	15 U.S.C. 1681n
Section 617	15 U.S.C. 1681o
Section 618	15 U.S.C. 1681p
Section 619	15 U.S.C. 1681q
Section 620	15 U.S.C. 1681r
Section 62l	15 U.S.C. 1681s
Section 622	15 U.S.C. 1681s-1
Section 623	15 U.S.C. 1681s-2
Section 624	15 U.S.C. 1681t
Section 625	15 U.S.C. 1681u
Section 626	15 U.S.C. 1681v
Section 627	15 U.S.C. 1681w
Section 628	15 U.S.C. 1681x
Section 629	15 U.S.C. 1681y

NOTICE TO USERS OF CONSUMER REPORTS UNDER CALIFORNIA CONSUMER CREDIT REPORTING AGENCIES ACT CIVIL CODE SECTION 1785.20-1785.22

The California Consumer Credit Reporting Agencies Act (Civil Code Sections 1785.1 – 1785.36) requires that this notice be provided to inform users of consumer reports of their responsibilities under Sections 1785.20-1785.22 of the California Civil Code.

Sections 1785.20-1785.22 impose the following duties upon users of consumer reports:

1785.20. (a) If any person takes any adverse action with respect to any consumer, and the adverse action is based, in whole or in part, on any information contained in a consumer credit report, that person shall do all of the following:

(1) Provide written notice of the adverse action to the consumer.

(2) Provide the consumer with the name, address, and telephone number of the consumer credit reporting agency which furnished the report to the person.

(3) Provide a statement that the credit grantor's decision to take adverse action was based in whole or in part upon information contained in a consumer credit report.

(4) Provide the consumer with a written notice of the following rights of the consumer:

(A) The right of the consumer to obtain within 60 days a free copy of the consumer's consumer credit report from the consumer credit reporting agency identified pursuant to paragraph (2) and from any other consumer credit reporting agency which compiles and maintains files on consumers on a nationwide basis.

(B) The right of the consumer under Section 1785.16 to dispute the accuracy or completeness of any information in a consumer credit report furnished by the consumer credit reporting agency.

(b) Whenever credit or insurance for personal, family, or household purposes involving a consumer is denied or the charge for such credit is increased either wholly or in part because of information obtained from a person other than a consumer credit reporting agency bearing upon consumer's credit worthiness or credit standing, the user of that information shall, within a reasonable period of time, and upon the consumer's written request for the reasons for that adverse action received within 60 days after learning of the adverse action, disclose the nature and substance of the information to the consumer. The user of the information shall clearly and accurately disclose to the consumer his or her right to make such a written request at the time the adverse action is communicated to the consumer.

(c) No person shall be held liable for any violation of this section if he or she shows by a preponderance of the evidence that at the time of the alleged violation he or she maintained reasonable procedures to assure compliance with this section.

(d) Nothing in this chapter shall excuse compliance with the requirements of Section 1787.2.

1785.20.1. (a) Except as provided in subdivision (b), any person who uses a consumer credit report in connection with any credit transaction not initiated by the consumer and which consists of a firm offer of credit shall provide with any solicitation made to the consumer a clear and conspicuous statement as to all of the following:

(1) Information contained in the consumer's prequalifying report was used in connection with the transaction.

(2) The consumer received the offer of credit, because the consumer satisfied the criteria for creditworthiness under which the consumer was selected for the offer.

(3) Where applicable, the credit may not be extended if, after the consumer responds to the offer, the consumer does not meet the criteria used to select the consumer for the offer.

(4) The consumer has a right to prohibit use of information contained in the consumer's file with any consumer credit reporting agency in connection with any credit transaction that is not initiated by the

consumer. The consumer may exercise this right by notifying the notification system or joint notification system established under subdivision (d) or (e) of Section 1785.11.

b) Subdivision (a) does not apply to any person using a prequalifying report if all of the following conditions are met:

(1) The person using the prequalifying report is affiliated by common ownership or common corporate control with the person who procured the report.

(2) The person who procures the prequalifying report from the consumer credit reporting agency clearly and conspicuously discloses to the consumer to whom the report relates, before the prequalifying report is provided to the person who uses the report, that the prequalifying report might be provided to, and used by, persons affiliated in the manner specified in paragraph (1) with the person that procured the report.

(3) The consumer consents in writing to this provision and use of the prequalifying report.

(c) No person shall be denied credit on the basis of the consumer's refusal to provide consent pursuant to paragraph (3) of subdivision (b), unless that consent is necessary for the extension of credit, related to that transaction, by an affiliate.

1785.20.2. Any person who makes or arranges loans and who uses a consumer credit score as defined in Section 1785.15.1 in connection with an application initiated or sought by a consumer for a closed end loan or establishment of an open end loan for a consumer purpose that is secured by one to four units of residential real property shall provide the following to the consumer as soon as reasonably practicable:

(a) A copy of the information identified in subdivision (a) of Section 1785.15.1 that was obtained from a credit reporting agency or was developed and used by the user of the information. In addition to the information provided to it by a third party that provided the credit score or scores, a lender is only required to provide the notice contained in subdivision (d).

(b) If a person who is subject to this section uses an automated underwriting system to underwrite a loan, that person may satisfy the obligation to provide a credit score by disclosing a credit score and associated key factors supplied by a consumer credit reporting agency. However, if a numerical credit score is generated by an automated underwriting system used by an enterprise, and that score is disclosed to the person, it shall be disclosed to the consumer consistent with subdivision (c). For purposes of this subdivision, the term "enterprise" shall have the meaning provided in paragraph (6) of Section 4502 of Title 12 of the United States Code.

(c) A person subject to the provisions of this section who uses a credit score other than a credit score provided by a consumer reporting agency may satisfy the obligation to provide a credit score by disclosing a credit score and associated key factors supplied by a consumer credit reporting agency.

(d) A copy of the following notice, which shall include the name, address, and telephone number of each credit bureau providing a credit score that was used:

NOTICE TO THE HOME LOAN APPLICANT

In connection with your application for a home loan, the lender must disclose to you the score that a credit bureau distributed to users and the lender used in connection with your home loan, and the key factors affecting your credit scores.

The credit score is a computer generated summary calculated at the time of the request and based on information a credit bureau or lender has on file. The scores are based on data about your credit history and payment patterns. Credit scores are important because they are used to assist the lender in determining whether you will obtain a loan. They may also be used to determine what interest rate you may be offered on the mortgage. Credit scores can change over time, depending on your conduct, how your credit history and payment patterns change, and how credit scoring technologies change.

Because the score is based on information in your credit history, it is very important that you review the credit-related information that is being furnished to make sure it is accurate. Credit records may vary from one company to another.

If you have questions about your credit score or the credit information that is furnished to you, contact the credit bureau at the address and telephone number provided with this notice, or contact the lender, if the lender developed or generated the credit score. The credit bureau plays no part in the decision to take any action on the loan application and is unable to provide you with specific reasons for the decision on a loan application.

If you have questions concerning the terms of the loan, contact the lender.

(e) This section shall not require any person to do the following:

(1) Explain the information provided pursuant to Section 1785.15.1.

(2) Disclose any information other than a credit score or key factor, as defined in Section 1785.15.1.

(3) Disclose any credit score or related information obtained by the user after a loan has closed.

(4) Provide more than one disclosure per loan transaction.

(5) Provide the disclosure required by this section when another person has made the disclosure to the consumer for that loan transaction.

(f) Any person's obligation pursuant to this section shall be limited solely to providing a copy of the information that was received from the consumer credit reporting agency. No person has liability under this section for the content of that information or for the omission of any information within the report provided by the consumer credit reporting agency.

(g) As used in this section, the term "person" does not include an "enterprise" as defined in paragraph (6) of Section 4502 of Title 12 of the United States Code.

1785.20.3. (a) Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, and who discovers that the consumer's first and last name, address, or social security number, on the credit application does not match, within a reasonable degree of certainty, the consumer's first and last name, address or addresses, or social security number listed, if any, on the consumer credit report, shall take reasonable steps to verify the accuracy of the consumer's first and last name, address, or social security number provided on the application to confirm that the extension of credit is not the result of identity theft, as defined in Section 1798.92.

(b) Any person who uses a consumer credit report in connection with the approval of credit based on an application for an extension of credit, and who has received notification pursuant to subdivision (k) of Section 1785.16 that the applicant has been a victim of identity theft, as defined in Section 1798.92, may not lend money or extend credit without taking reasonable steps to verify the consumer's identity and confirm that the application for an extension of credit is not the result of identity theft.

(c) Any consumer who suffers damages as a result of a violation of this section by any person may bring an action in a court of appropriate jurisdiction against that person to recover actual damages, court costs, attorney's fees, and punitive damages of not more than thirty thousand dollars ($30,000) for each violation, as the court deems proper.

(d) As used in this section, "identity theft" has the meaning given in subdivision (b) of Section 1798.92.

(e) For the purposes of this section, "extension of credit" does not include an increase in an existing open-end credit plan, as defined in Regulation Z of the Federal Reserve System (12 C.F.R. 226.2), or any change to or review of an existing credit account.

(f) If a consumer provides initial written notice to a creditor that he or she is a victim of identity theft, as defined in subdivision (d) of Section 1798.92, the creditor shall provide written notice to the consumer of his or her rights under subdivision (k) of Section 1785.16.

(g) The provisions of subdivisions (k) and (l) of Section 1785.16 do not apply to a consumer credit reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the database of another consumer credit reporting agency or the databases of multiple consumer credit reporting agencies, and does not maintain a permanent database of credit information from which new credit reports are produced.

(h) This section does not apply if one of the addresses at issue is a United States Army or Air Force post office address or a United States Fleet post office address.

1785.20.5. (a) Prior to requesting a consumer credit report for employment purposes, the user of the report shall provide written notice to the person involved. The notice shall inform the person that a report will be used and the source of the report, and shall contain a box that the person may check off to receive a copy of the credit report. If the consumer indicates that he or she wishes to receive a copy of the report, the user shall request that a copy be provided to the person when the user requests its copy from the credit reporting agency. The report to the user and to the subject person shall be provided contemporaneously and at no charge to the subject person.

(b) Whenever employment involving a consumer is denied either wholly or partly because of information contained in a consumer credit report from a consumer credit reporting agency, the user of the consumer credit report shall so advise the consumer against whom the adverse action has been taken and supply the name and address or addresses of the consumer credit reporting agency making the report. No person shall be held liable for any violation of this section if he or she shows by a preponderance of the evidence that, at the time of the alleged violation, he or she maintained reasonable procedures to assure compliance with this section.

1785.21. (a) A user in its discretion may notify the consumer that upon request the user may contact the consumer reporting agency and request that the consumer reporting agency investigate the current status of an item or items of information contained in the consumer report if the consumer disputes the completeness or accuracy of an item or items of information as provided to the user.

(b) The consumer credit reporting agency may require identification from the user to insure the validity of the request and, in that regard, may require that the request be put in writing with proper identification.

(c) In the event that any such request is made and identification given in the form or manner demanded by the consumer credit reporting agency, such agency shall review the file of the consumer and report the current status of the disputed information to the user and the consumer by the most expeditious means possible.

(d) No user who furnishes information pursuant to this section shall be liable to any person for furnishing such information.

1785.22. (a) A person may not procure a consumer credit report for the purpose of reselling the report or any information therein unless the person discloses to the consumer credit reporting agency which issues the report the identity of the ultimate end user and each permissible purpose for which the report is furnished to the end user of the consumer credit report or information therein.

(b) A person that procures a consumer credit report for the purpose of reselling the report or any information therein shall do all of the following:

(1) Establish and comply with reasonable procedures designed to ensure that the consumer credit report or information is resold by the person only for a purpose for which the report may be furnished under this title. These procedures shall include all of the following:

(A) Identification of each prospective user of the resold consumer credit report or information.

(B) Certification of each purpose for which the consumer credit report or information will be used.

(C) Certification that the consumer credit report or information will be used for no other purpose.

(2) Before reselling the consumer credit report or information, the person shall make reasonable efforts to verify the identities and certifications made under paragraph (1).

All furnishers subject to the Federal Trade Commission's jurisdiction must comply with all applicable regulations, including regulations promulgated after this notice was prescribed in 2004. Information about applicable regulations currently in effect can be found at the Commission's Web site, www.ftc.gov/credit. Furnishers who are not subject to the Commission's jurisdiction should consult with their regulators to discern any relevant regulations.

NOTICE TO FURNISHERS OF INFORMATION: OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The federal Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681-1681y, imposes responsibilities on all persons who furnish information to consumer reporting agencies (CRAs). These responsibilities are found in Section 623 of the FCRA, 15 U.S.C. 1681s-2. State law may impose additional requirements on furnishers. All furnishers of information to CRAs should become familiar with the applicable laws and may want to consult with their counsel to ensure that they are in compliance. The text of the FCRA is set forth in full at the Web- site of the Federal Trade Commission (FTC): www.ftc.gov/credit. A list of the sections of the FCRA cross referenced to the U.S. Code is at the end of this document.

Section 623 imposes the following duties upon furnishers:

ACCURACY GUIDELINES

The banking and credit union regulators and the FTC will promulgate guidelines and regulations dealing with the accuracy of information provided to CRAs by furnishers. The regulations and guidelines issued by the FTC will be available at www.ftc.gov/credit when they are issued. Section 623(e).

GENERAL PROHIBITION ON REPORTING INACCURATE INFORMATION

The FCRA prohibits information furnishers from providing information to a CRA that they know or have reasonable cause to believe is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. Sections 623(a)(1)(A) and (a)(1)(C).

DUTY TO CORRECT AND UPDATE INFORMATION

If at any time a person who regularly and in the ordinary course of business furnishes information to one or more CRAs determines that the information provided is not complete or accurate, the furnisher must promptly provide complete and accurate information to the CRA. In addition, the furnisher must notify all CRAs that received the information of any corrections, and must thereafter report only the complete and accurate information. Section 623(a)(2).

DUTIES AFTER NOTICE OF DISPUTE FROM CONSUMER

If a consumer notifies a furnisher, at an address specified for the furnisher for such notices, that specific information is inaccurate, and the information is, in fact, inaccurate, the furnisher must thereafter report the correct information to CRAs. Section 623(a)(1)(B).

If a consumer notifies a furnisher that the consumer disputes the completeness or accuracy of any information reported by the furnisher, the furnisher may not subsequently report that information to a CRA without providing notice of the dispute. Section 623(a) (3).

The federal banking and credit union regulators and the FTC will issue regulations that will identify when an information furnisher must investigate a dispute made directly to the furnisher by a consumer. Once these regulations are issued, furnishers must comply with them and complete an investigation within 30 days (or 45 days, if the consumer later provides relevant additional information) unless the dispute is frivolous or irrelevant or comes from a "credit repair organization." The FTC regulations will be available at www.ftc.gov/credit. Section 623(a)(8).

DUTIES AFTER NOTICE OF DISPUTE FROM CONSUMER REPORTING AGENCY

If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

1. Conduct an investigation and review all relevant information provided by the CRA, including information given to the CRA by the consumer. Sections 623(b)(1)(A) and (b)(1)(B).
2. Report the results to the CRA that referred the dispute, and, if the investigation establishes that the information was, in fact, incomplete or inaccurate, report the results to all CRAs to which the furnisher provided the information that compile and maintain files on a nationwide basis. Section 623(b)(1)(C) and (b)(1)(D)3. Complete the above steps within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). Section 623(b)(2).

3. Complete the above steps within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). Section 623(b)(2).
4. Promptly modify or delete the information, or block its reporting. Section 623(b)(1)(E).

DUTY TO REPORT VOLUNTARY CLOSING OF CREDIT ACCOUNTS

If a consumer voluntarily closes a credit account, any person who regularly and in the ordinary course of business furnishes information to one or more CRAs must report this fact when it provides information to CRAs for the time period in which the account was closed. Section 623(a)(4).

DUTY TO REPORT DATES OF DELINQUENCIES

If a furnisher reports information concerning a delinquent account placed for collection, charged to profit or loss, or subject to any similar action, the furnisher must, within 90 days after reporting the information, provide the CRA with the month and the year of the commencement of the delinquency that immediately preceded the action, so that the agency will know how long to keep the information in the consumer's file. Section 623(a)(5).

Any person, such as a debt collector, that has acquired or is responsible for collecting delinquent accounts and that reports information to CRAs may comply with the requirements of Section 623(a)(5) (until there is a consumer dispute) by reporting the same delinquency date previously reported by the creditor. If the creditor did not report this date, they may comply with the FCRA by establishing reasonable procedures to obtain and report delinquency dates, or, if a delinquency date cannot be reasonably obtained, by following reasonable procedures to ensure that the date reported precedes the date when the account was placed for collection, charged to profit or loss, or subjected to any similar action. Section 623(a)(5).

DUTIES OF FINANCIAL INSTITUTIONS WHEN REPORTING NEGATIVE INFORMATION

Financial institutions that furnish information to "nationwide" consumer reporting agencies, as defined in Section 603(p), must notify consumers in writing if they may furnish or have furnished negative information to a CRA. Section 623(a)(7). The Federal Reserve Board has prescribed model disclosures, 12 CFR Part 222, App. B.

DUTIES WHEN FURNISHING MEDICAL INFORMATION

A furnisher whose primary business is providing medical services, products, or devices (and such furnisher's agents or assignees) is a medical information furnisher for the purposes of the FCRA and must notify all CRAs to which it reports of this fact. Section 623(a)(9). This notice will enable CRAs to comply with their duties under Section 604(g) when reporting medical information.

DUTIES WHEN ID THEFT OCCURS

All furnishers must have in place reasonable procedures to respond to notifications from CRAs that information furnished is the result of identity theft, and to prevent refurnishing the information in the future. A furnisher may not furnish information that a consumer has identified as resulting from identity theft unless the furnisher subsequently knows or is informed by the consumer that the information is correct. Section 623(a)(6). If a furnisher learns that it has furnished inaccurate information due to identity theft, it must notify each consumer reporting agency of the correct information and must thereafter report only complete and accurate in- formation. Section 623(a)(2). When any furnisher of information is notified pursuant to the procedures set forth in Section 605B that a debt has resulted from identity theft, the furnisher may not sell, transfer, or place for collection the debt except in certain limited circumstances. Section 615(f).

The FTC's Web site, www.ftc.gov/credit, has more information about the FCRA, including publications for businesses and the full text of the FCRA.