Verification Services

PNC's Verification Services ("Service") enables the customer to submit verification inquiries to help confirm information about their intended payment counterparties and the counterparties' bank accounts. This Service accesses information maintained by Early Warning (defined below) and other data providers and sources. Capitalized terms used herein and not otherwise defined herein or in the Treasury Management Services Agreement ("TMSA") shall have the definitions given such terms on *Exhibit A*. The Service is more particularly described on *Exhibit B* attached hereto and made a part hereof. By using this Service, the customer must comply with the following terms.

I. GENERAL

PNC Obligations:

- PNC will enable access to the Service via one or more supported delivery channels, as implemented by PNC based on the customer's express request.
- In response to each verification inquiry, the Service will provide the customer with information regarding the intended payment counterparties and the counterparties' bank accounts that are the subject of the inquiry ("Response Data"), which is provided on an "as is" and "as available" basis.
- PNC MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS SERVICE.

Customer Obligations:

- For all Services, the customer must comply with all Applicable Laws, regulations and other requirements, including but not limited to the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act (GLBA).
- Customer must comply with all the provisions of this Schedule.
- Customer must promptly provide to PNC any requested documentation, implementation forms, due diligence or similar items. Without limiting the generality of the foregoing, Customer agrees to furnish PNC, at PNC's request, such other information and documentation related to Customer or the use of the Service as may reasonably be requested by PNC from time to time, for purposes of compliance by PNC with Applicable Laws, and any policy or procedure implemented by PNC to comply therewith, or responding to any request for information relating to the Service.
- If data providers or sources require compliance with specific rules or technical conditions, PNC will inform the customer of such, and the customer must adhere to these rules and conditions.

Compliance:

- The customer will not use this Service for any unlawful or unpermitted purpose. The customer will comply with the Documentation that will identify additional requirements for this Service.
- The customer will be responsible for the customer's use of Response Data. The customer agrees that the customer is the end user of the Response Data and will not provide Response Data to any other person or entity, such as the customer's own customer, for the customer's customer to

use. The customer may not sell, resell, sublicense or otherwise transfer any part of the Response Data to any other person or entity. PNC reserves the right to decline to provide Response Data if PNC believes such Response Data will be used in a manner that is not compliant with Applicable Law.

- If customer is using the Service in conjunction with the U.S. Department of the Treasury Bureau of the Fiscal Service Treasury Check Verification System (www.tcvs.fiscal.treasury.gov), the customer acknowledges receipt of the notice provided on *Exhibit H* attached hereto.
- If the customer is a "retail seller" as defined in Section 1802.3 of the California Civil Code, the customer warrants that it will not submit a request for Response Data in connection with issuing credit to a consumer who appears in person on the basis of an application for credit submitted in person.

Inquiries:

- The customer may initiate a specific Inquiry for the Service in accordance with the authorized uses and the Documentation via one or more supported delivery channels, as implemented by PNC based on the customer's express request.
- After the customer submits an Inquiry, if there is a Match, the customer will receive Response Data from PNC.

Response Data and the Customer's Responsibility:

- The Response Data may include (as applicable and available):
    - Bank account status Match response about supported accounts from financial institutions, bank account ownership and authority Match response, and related details;
    - Identity verification Match information and related details;
    - Email address verification Match information and related details.
- The Response Data is time-sensitive, as of a point in time, and only permitted to be used in connection with the specific Inquiry for which it was requested.
- The Response Data is provided on an "as is" and "as available" basis. This Service is for the customer's informational purposes only and the customer is solely responsible for decisions the customer makes based on this information. Customer's decision with respect to any payment or account should not be made solely on the Response Data.
- PNC MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS SERVICE.

II. SPECIFIC SERVICE TERMS

a. Bank Account Verification (Early Warning) Services

Eligibility:

- A customer may apply to participate in the National Shared Database or receive Early Warning Services if it meets the criteria set forth in the Documentation or is otherwise appropriately approved by Early Warning.
- In order to use such Services, Customer must be domiciled in the United States of America or its Territories.

FCRA Services:

The customer understands and agrees that if it uses the Bank Account Verification Services that are subject to FCRA, it will comply with the additional requirements set forth on *Exhibit C*.

Flow Downs:

In connection with its use of the Bank Account Verification Services, Customer also agrees to comply with the terms provided by Early Warning set forth on *Exhibit D* (the “Flow Downs”). In the event of a conflict between the Flow Downs and this Schedule with respect to the Bank Account Verification Services, the Flow Downs shall control.

Bank Account Contribution:

- Participants that are Financial Institutions or Financial Services Companies and have 100,000 or more Accounts and use any Early Warning Service must contribute all required data sets, pursuant to all relevant Documentation.
- Participant acknowledges receipt of the notice to furnishers provided by PNC , which describes the obligations of persons who furnish information to consumer reporting agencies and agrees to comply with such obligations regarding Contribution.

b. Identity and Email Verification Services

The customer certifies that because the information provided in the “ID Business,” “ID Consumer,” “ID Consumer with KBA,” and “Email and Social Intelligence” services is not consumer report information, the customer will not request or use the Service as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes, employment purposes, tenant screening or for any other purpose authorized under the FCRA or similar state or local statute, rules or regulations.

Permissible Purpose. The customer certifies that it will order and use the “ID Consumer” and “ID Consumer with KBA” services in connection with the following use involving the subject of the report and for no other use:

To use in the ordinary course of business to verify the accuracy of information submitted by the consumer to protect against or prevent actual fraud, unauthorized transactions, claims or other liability.

EXHIBIT A

Definitions

Certain Definitions Applicable to the Service:

- "Account" means an account at a bank or credit union from which the accountholder is permitted to make transfers or withdrawals, with or without notice, by any means. Includes "transaction accounts," as defined by the Board of Governors of the Federal Reserve System in Regulation CC, 12 C.F.R. § 204.2(e).
- "Applicable Law(s)" with respect to any entity, means any federal, state, or local statute, rule, regulation, or other law or requirement imposed by any governmental authority that applies to such entity, and including without limitation, FCRA and GLBA.
- "Authorized Use(s)" means the authorized use of the Service as permitted by the Documentation and, with respect to the Early Warning Services, as further described in *Exhibits F & G* attached hereto, as may be amended from time to time.
- "Contribute" or "Contribution" means the transmittal of data by customers to Early Warning to populate to the National Shared Database.
- "Contributed Data" means the specific data elements, as specified in the Documentation, which are contributed by a customer to the National Shared Database.
- "Documentation" means applicable requirements of the Operating Rules, system requirements, user guides referenced herein, technical specifications, release notes, and other materials made available by PNC, Early Warning (if and as applicable) and any other data provider or source, that describe the permitted use of, or are used in connection with, the Service.
- "Early Warning" means Early Warning Services, LLC, a Delaware limited liability company.
- "Early Warning Service" or "EWS Service" for purposes of this Schedule means the services described in Section II.a. and *Exhibits F & G* of this Schedule.
- "EWS Participant" or "Participant" for purposes of this Schedule means an entity that receives the EWS Service(s) pursuant to the eligible categories set forth on *Exhibit E* and in the Operating Rules and as further described in the Documentation. A Participant is the end user of the Response Data. All Participants are Customers for purposes of this Schedule.
- "FCRA" means the federal Fair Credit Reporting Act, set forth in 15 U.S.C. §§ 1681 et seq., all implementing regulations and any equivalent state statute.
- "GLBA" means the Gramm-Leach-Bliley Act, set forth in 15 U.S.C. §§ 6801 et seq. and all implementing regulations.
- "Inquiry" means a request by an Inquirer for Response Data pursuant to the Service. The information contained within an Inquiry ("Inquiry Data") may be described in the applicable Documentation.
- "Inquirer" means an entity that meets the eligibility requirements of the Documentation and receives Response Data. All Inquirers are customers for purposes of this Schedule.

- “Match” means the occurrence of when data elements contained within an Inquiry match against data elements contained within one or more verification data sources.
- “Merged Response Data” means information that PNC is permitted to provide to a Participant as part of the Service that includes Early Warning Response Data and other data or information obtained or maintained by PNC from sources other than Early Warning, represented in one value.
- “National Shared Database” means the collection of Contributed Data maintained by Early Warning in one or more databases.
- “National Shared Database Operating Rules,” “Operating Rules” or “Rules” means the National Shared Database Operating Rules governing Early Warning’s role as a trusted custodian of, and an eligible Participant’s participation in, the National Shared Database, as amended from time to time in accordance thereof.
- “Services Agreement” means the TMSA, this Schedule and any other terms and conditions applicable to the Service.
- “Translated Response Data” means Response Data that is translated into a decision for a Participant (e.g., “Pass,” “Decline”) at the direction of Early Warning or another data provider, as applicable.
- “Use Case” means each authorized use of Contributed Data prescribed in the Rules.

EXHIBIT B

Service Description

Service	Description
Bank Account Verification	
Verify	This service allows you to find out if a domestic bank account exists, check its status, and get key details like account type, maturity standing, and supported payment types.
Verify and Authenticate	This service allows you to verify if a known domestic bank account is active, who owns it or has signing authority, and provides details like account type, maturity standing and supported payment types.
Validate	This service allows you to find out if a domestic bank account exists, check its status and allows you to learn about supported payment types.
Validate and Authenticate	This service allows you to validate if a known domestic bank account is active, who owns it or has signing authority, and allows you to learn about supported payment types.
Identity Verification	
ID Business	This service allows you to confirm a business's existence and true identity and learn about related details based on the best-matched business record and any alerts, if present.
ID Consumer	This service allows you to confirm a consumer's existence and true identity and learn about related details based on the best-matched consumer record and any alerts, if present.
ID Consumer with KBA (API only)	This service allows you to confirm a consumer's existence and true identity through knowledge-based authentication (KBA) questions presented in a consumer-facing enrollment workflow.
Email Verification	
Email and Social Intelligence	This service allows you to check if an email address exists and provides useful details like who it belongs to, their job title, the company and domain its linked to, and any connected social media profiles.

EXHIBIT C

Additional Terms for FCRA-Related Bank Account Verification Services

1. If customer uses any portion of the Service that provides consumer reports subject to FCRA, the customer will only obtain a consumer report if the customer has a permissible purpose to obtain and use the report pursuant to the FCRA. The customer certifies that the consumer reports provided hereunder may be requested and used only if the customer has a legitimate business need for the information in connection with a business transaction that is initiated by the consumer, or the customer obtains the express written authorization of the consumer to obtain the consumer report. The customer certifies that it will request and use the consumer reports for no other purpose.
2. If Verify is selected, customer agrees that it will use the consumer report solely:
    a. To validate the existence of an account and all associated data in determining whether to accept or decline a check or automated clearinghouse entry (each 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.
    e. To determine whether to allow the 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.
3. If Authenticate is selected and used with Verify, the customer further agrees that it will use the consumer report solely:
    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 account holder, user or signatory of the Account on which such 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 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.
    e. To determine whether to allow an account to be enrolled for use in connection with future transactions by validating that the consumer is an authorized accountholder, user or signatory of the account.
    f. UNDER SECTION 619 OF THE FCRA, ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18, UNITED STATES CODE, IMPRISIONED FOR NOT MORE THAN 2 YEARS, OR BOTH.

4. Documentation of Permissible Purpose for Verify and Authenticate. The customer certifies that it will rely upon, and retain, the following documentation and/or authorization from consumers as evidence of the customer's permissible purpose:
    a. Physical Check presented by consumer.
    b. Electronic signature of consumer.
    c. Written Authorization from the consumer (on signed application).
    d. Written Authorization (by recorded voice authorization).
5. Notice of Adverse Action and Consumer Dispute Process:
    a. The customer understands and agrees that under the FCRA, as a user of the consumer report, the customer must provide notice of adverse action in compliance with Section 615 of the FCRA when the consumer report information provided by PNC serves as the basis for the customer's declination. The notice must include contact information for Early Warning.
    b. Should a consumer contact Early Warning in response to a notice of adverse action or to dispute information furnished by the customer, customer acknowledges and agrees that Early Warning may be required to provide additional information regarding the customer. If the customer is a furnisher, the customer will conduct a timely investigation of the dispute and meet FCRA requirements for responding to disputes. If required under the FCRA or requested by a consumer for any reason, the customer has identified contact information regarding the customer's name, address and phone number to be provided by Early Warning to consumers. Should the customer's contact information change, the customer must notify PNC and Early Warning promptly in writing.
6. Notice to Users: Customer acknowledges receipt of the Notice to Users of Consumer Reports attached hereto as *Exhibit I*.

EXHIBIT D

Flow Downs – Bank Account Verification Services

- The following Flow Downs apply to all Participants, unless otherwise noted below with respect to Translated Response Data:
  - Upon request by Participant, Early Warning will provide to Participant a copy of its most recent Annual Risk Report ("ARR"). If, in addition to the information in the ARR, Participant requires to conduct an on-site audit of Early Warning's information security program, Participant may attend one of Early Warning's regularly scheduled consolidated on-site audits at no charge (expenses are the Participant's responsibility). Any on-site audits outside of the regularly scheduled consolidated on-site audit periods may be requested for a daily fee to be agreed by Early Warning and the Participant. 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. If Participant requires that Early Warning complete a questionnaire regarding Early Warning's information security program, then a fee shall be assessed to Participant for the questionnaire, as agreed upon by Early Warning and the Participant. Fees related to such audits or questionnaires will be billed to Participant separately from fees for the EWS Service(s).
  - Participant shall not knowingly permit any of its directors, officers, employees, contractors, subcontractors, attorneys, auditors and accountants, to access the EWS Service(s) if the person has been convicted of a crime in connection with: (a) 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 (b) a felony.
  - Early Warning may suspend provision of the EWS Service(s) for a Participant, upon written notice to PNC and Participant, if Participant does not comply with the requirements of the Services Agreement, the Documentation, and these Flow Downs, or if Early Warning is unable to verify Participant's compliance with the requirements of the Services Agreement, Flow Downs and Documentation including the Authorized Use(s) in *Exhibits F & G*.
  - Early Warning may cease providing Response Data to Participant if Participant is associated with a security breach or any fraudulent or illegal conduct which, in Early Warning' good faith determination, materially harms Participant's general reputation or would harm Early Warning's reputation by its continued association with Participant.
  - Participant shall use the Response Data only for the Authorized Uses.
  - Participant agrees that Response Data is time sensitive and shall only be used in connection with the specific Inquiry for which it was requested.
  - Participant shall not merge, aggregate, or compile Response Data into any other database for use in connection with future Inquiries. Participant shall not transmit Response Data received in response to an Inquiry to any party other than in response to an Inquiry initiated by such Participant. Without limitation to the foregoing, Participant shall not allow any third party to access the Response Data. Participant shall not sell, resell, sublicense, or otherwise transfer any part of the Response Data to any other person or entity other than the Participant.

- Participant shall prohibit any customer of Participant that receives a Response that is comprised of or derived from, in whole or in part, Response Data, from selling, reselling, sublicensing, or otherwise transferring any part of such response to any other person or entity, unless approved in writing by Early Warning. Early Warning may limit or prohibit the markets and/or types of businesses that are eligible to receive a response that is comprised of or derived from, in whole or in part, Response Data.
- Early Warning is a third-party beneficiary of the Services Agreement as it relates to the Flow Downs and Early Warning retains the right to enforce the terms of the Flow Downs against the Participant.
- Early Warning shall have no liability arising out of any Services Agreement between PNC and any Participant, including, without limitation, any duties, or obligations (contractual, at law or otherwise) owed by PNC to any Participant or by any Participant to PNC under the Services Agreement.
- Participant shall maintain a written information security program that contains administrative, technical and physical safeguards designed to: (a) ensure the security and confidentiality of Response Data; (b) protect against any anticipated threats or hazards to the security or integrity of Response Data; (c) protect against unauthorized access to or use of such Response Data that could result in substantial harm or inconvenience to any customer or Participant; (d) limit access, use and disclosure of Response Data as expressly permitted by this Service Agreement; (e) ensure the proper disposal of Response Data, (f) ensure the encryption of Response Data at rest using a current industry acceptable encryption method (e.g., AES-256 or stronger encryption); and (g) comply with Applicable Law. Participant's information security program must be designed to: (i) meet the objectives of the Interagency Guidelines Establishing Information Security Standards promulgated by the federal banking agencies as amended from time to time, and (ii) include control objectives that meet applicable industry standards such as ISO 27002, FFIEC, OCC, PCI, or NIST. Participant will promptly notify Early Warning of any material modification to Participant's information security program but only as it relates to the protection of Response Data. ***Not required for Participants that only receive Translated Response Data (i.e., Merchants).***
- Early Warning shall have the right, during normal business hours, upon reasonable advance notice, and not more than once per calendar year, to conduct a virtual online audit of Participants' information security program and related policies, controls, processes, and procedures. In addition, Participant shall complete a Shared Assessment Significant Information Gathering (SIG) Questionnaire OR provide to Early Warning, upon request, a copy of its 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 its external auditors related to the EWS Services or Reseller Services, as applicable. ***Not required for Participants that only receive Translated Response Data (i.e., Merchants).***
- In the event of a breach in security resulting in actual or suspected loss of or unauthorized access to Response Data, Participant shall: (a) immediately notify Early Warning by calling (877) 275-7774, Option 4; (b) conduct a forensics examination to determine to what extent Data was compromised; (c) provide to Early Warning, in writing,

details concerning the breach, including: (i) nature and impact of the breach, (ii) assessment of immediate risk due to the breach, (iii) corrective actions already taken, and (iv) corrective actions to be taken; (d) cooperate with Early Warning and any affected Inquirers, Contributors, 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 (e) take measures to restore and enhance its security policies and procedures to avoid further breaches. ***Not required for Participants that only receive Translated Response Data (i.e., Merchants).***

  - Early Warning shall have the right, during normal business hours, and not more than once per calendar year, and upon reasonable advance notice, to conduct an online virtual review with Participant to verify Participant's compliance with these Flow Downs, the Services Agreement and/or the Documentation, as applicable to that Participant.

- The following Flow Downs apply to all Participants <u>except</u> Government Entities:

  - Participant acknowledges and agrees that Early Warning may use Inquiry Data for the purpose of: (a) providing the EWS Service(s); (b) preparing statistical reports and conducting data analytics, parsing routines, data modeling, and other analyses to test and evaluate services provided by Early Warning, provided that such reports and analyses do not identify Participant as the source of any specific Inquiry Data; (c) developing and providing new services or enhancements to existing services provided by Early Warning, provided that in such use, specific Inquiry Data is not associated with or identifiable as having been received from Participant; (d) 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, and; (e) retention as required by Applicable Law and as necessary for reasonable record keeping purposes pursuant to Early Warning's record retention policies.

- The following Flow Downs apply to Financial Institution ("FI") Participants only:

  - Participant acknowledges and agrees that Early Warning will use Contributed Data for the purpose of providing the EWS Service(s) and other purposes as set forth in the Documentation.

  - FI Participants shall be bound to the requirements described in the Documentation applicable to the Participant Category and EWS Service(s).

- The following Flow Downs apply to all Participants using "Verify" and "Verify and Authenticate" (FCRA-Governed Services):

  - If the Participant uses Response Data to take adverse action against the consumer about whom the Response Data relates, the Participant agrees to refer such consumer to Early Warning for handling disputes concerning the completeness or accuracy of any item of information contained within the Response Data. Participant shall comply with all applicable provisions of the FCRA and any state equivalent in handling such disputes making such disclosures.

  - If the Participant uses Merged Response Data to take adverse action against the consumer about whom the Merged Response Data relates, the Participant agrees to refer such consumer to Early Warning for handling disputes concerning the completeness or accuracy of any item of information contained within the Merged Response Data and for disclosure of each consumer reporting agency that was used to provide information in the Merged Response Data. Participant shall comply with all applicable provisions of the FCRA and any state equivalent in handling such disputes making such disclosures.

EXHIBIT E

EWS Participant Categories

The following categories of Participants are eligible to participate in the National Shared Database or receive Services from Early Warning, subject to specific Use Case requirements:

- **Financial Institution (FI):** An insured retail or commercial bank or credit union, chartered under the laws of the United States or any State or the Territories, engaged in the business of receiving deposits, managing withdrawals and making loans.
- **Financial Services Company (FSC):** An entity that offers one or more of the following financial services or products and are subject to regulation and supervision by applicable federal or state authorities of the United States or Territories: lending, insurance or broker-dealer.
- **Payment Processing Company (PPC):** An entity that uses the Services in connection with providing one or more of the following payment processing services to Financial Institutions, Financial Services Companies, Merchants or Government Entities: check acceptance and guarantee, check collection, remittance processing, check printing, bill payment, payroll, acquirer processing, disbursements.
- **Merchant (Merch):** An entity (including a nonprofit organization) that accept Items as payment from or remit Items as payment to Consumers or Companies in connection with the goods or services offered or provided by such entity.
- **Identity Theft Protection Service Provider (IDSP):** An entity that offers identity theft protection services to Consumer subscribers.
- **Government Entity (Govt):**
    - A local, state and federal government agency of the United States or the Territories and their contractors; or
    - A Government-Sponsored Enterprise (GSE) - A privately held corporation with public purposes created by the U.S. Congress to reduce the cost of capital for certain borrowing sectors of the economy. Members of these sectors include students, farmers, and homeowners. Examples of government-sponsored enterprises s include: Federal Home Loan Bank, Federal National Mortgage Association (Fannie Mae), Federal Home Loan Mortgage Corporation (Freddie Mac), Federal Farm Credit Bank and the Resolution Funding Corporation.

EXHIBIT F

DESCRIPTION OF THE EARLY WARNING SERVICES AND AUTHORIZED USES

Service Name	**Validate, Validate and Authenticate**
Service Description	Validates account ownership (that the recipient or the initiator of a payment, as the case may be, is the owner of or authorized to transact on the bank account which the payment is being deposited into or is being drawn from, as the case may be), and status of an Account (to confirm whether the bank account is open or closed).
Authorized Use(s) of Service	**Merchants:** • Determine whether to accept an Item for payment, initiate an Item for payment or enroll an Account for the purpose of accepting or initiating Items for payment in the future in connection with goods or services offered or provided by the Participant; and • Validate that (1) the Consumer is an authorized accountholder, user or signatory of the Account, or (2) the Company name is associated with the Account. **Government Entities:** • Determine whether to accept an Item for payment, initiate an Item for payment or enroll an Account for the purpose of accepting or initiating Items for payment in the future; and • Validate that (1) the Consumer is an authorized accountholder, user or signatory of the Account, or (2) the Company name is associated with the Account. **Other Participants:** • Determine whether to accept an Item for payment, initiate an Item for payment or enroll an Account for the purpose of accepting or initiating Items for payment in the future; and • Validate that (1) the Consumer is an authorized accountholder, user or signatory of the Account, or (2) the Company name is associated with the Account; and • Validate the status of an Account in determining whether to process a check order.
Inquiry & Response Data	As set forth in the technical specifications and/or user guides, which are included in the Documentation.
Response Data Format	As set forth in the technical specifications and/or user guides, which are included in the Documentation.

FCRA Applicability	The "Validate" and "Validate and Authenticate" service is not a "consumer report" as defined in 15 U.S.C. §1681a(d) of the Fair Credit Reporting Act ("FCRA") (15 U.S.C. 1681 *et seq*.) and is not provided to be used, and shall not be used, as a factor in determining a consumer's eligibility for any purpose covered by the FCRA.

EXHIBIT G

DESCRIPTION OF THE EARLY WARNING SERVICES AND AUTHORIZED USES (CONT.)

<table>
<tr><th>Service Name</th><th>Verify, Verify and Authenticate</th></tr>
<tr><td>Service Description</td><td>Screens check and ACH payments to determine the likelihood the payment will return by validating the existence and status of an account.</td></tr>
<tr><td>Authorized Use(s) of Service</td><td>Merchants:
Determine whether to accept an Item for payment, initiate an Item for payment or enroll an Account for the purpose of accepting or initiating Items for payment in the future in connection with goods or services offered or provided by the Participant; and
Validate that (1) the Consumer is an authorized accountholder, user or signatory of the Account, or (2) the Company name is associated with the Account.
Government Entities:
Determine whether to accept an Item for payment, initiate an Item for payment or enroll an Account for the purpose of accepting or initiating Items for payment in the future; and
Validate that (1) the Consumer is an authorized accountholder, user or signatory of the Account, or (2) the Company name is associated with the Account.
Other Participants:
Determine whether to accept an Item for payment, initiate an Item for payment or enroll an Account for the purpose of accepting or initiating Items for payment in the future; and
Validate that (1) the Consumer is an authorized accountholder, user or signatory of the Account, or (2) the Company name is associated with the Account; and
As a factor in verifying or guaranteeing an Item; and
Determine whether to delay or restrict the open to buy decision.</td></tr>
<tr><td>Inquiry & Response Data</td><td>As set forth in the technical specifications and/or user guides, which are included in the Documentation.</td></tr>
<tr><td>Response Data Format</td><td>As set forth in the technical specifications and/or user guides, which are included in the Documentation.</td></tr>
</table>

FCRA Applicability	The "Verify" and "Verify and Authenticate" service is a "consumer report" as defined in 15 U.S.C. §1681a(d) of the Fair Credit Reporting Act ("FCRA") (15 U.S.C. 1681 *et seq*.) and may only be used purposes covered by the FCRA. Reseller acknowledges receipt of the Notice to Users of Consumer Reports; Obligations Under the FCRA and Notices to Furnishers of Information; Obligations of Furnishers Under the FCRA, as set forth in the Documentation (the "FCRA Notices"), which shall be provided to Participants using "Verify" or "Verify and Authenticate."

EXHIBIT H

NOTICE TO TREASURY CHECK VERIFICATION SYSTEM (TCVS) USERS

EARLY WARNING HAS ESTABLISHED AN INTERFACE TO THE U.S. DEPARTMENT OF THE TREASURY, BUREAU OF THE FISCAL SERVICE TREASURY CHECK VERIFICATION SYSTEM (TCVS), TO VALIDATE U.S. TREASURY CHECKS. EARLY WARNING IS REQUIRED TO PROVIDE ALL PARTICIPANTS WHO WILL UTILIZE THIS SERVICE WITH THE FOLLOWING INFORMATION:

IMPORTANT NOTICE

- **BE ADVISED THAT ACCESS TO THE TREASURY CHECK VERIFICATION SYSTEM PROVIDED THROUGH THIS SERVICE ENHANCEMENT IS DESIGNED TO PROVIDE YOU WITH INFORMATION TO ASSIST IN MAKING A DECISION REGARDING THE VALIDITY OF A TREASURY CHECK, AND THAT THE DETERMINATION ON WHETHER TO NEGOTIATE A TREASURY CHECK REMAINS YOUR SOLE RESPONSIBILITY. WHILE TREASURY WILL MAKE REASONABLE EFFORTS TO ENSURE THE ACCURACY OF THE DATA AVAILABLE IN THE TREASURY CHECK VERIFICATION SYSTEM, INFORMATION MAY NOT BE TIMELY SINCE IT IS UPDATED ONCE A DAY (NOT IN REAL TIME). BY USING THIS SERVICE ENHANCEMENT, YOU ACKNOWLEDGE THAT NEITHER TREASURY NOR EARLY WARNING SERVICES WARRANTS THE ACCURACY OR TIMELINESS OF THE DATA, OR ACCEPTS ANY LIABILITY FOR ANY INACCURACIES IN THAT DATA. YOU FURTHER ACKNOWLEDGE THAT ACCESS TO THIS SERVICE ENHANCEMENT MAY BE REVOKED AT ANY TIME, IMMEDIATELY, UPON EMAIL NOTIFICATION TO YOU.**

EXHIBIT I

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

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.