WESTERN VIRGINIA
WATER AUTHORITY

Western Virginia Water Authority Identity Theft Prevention Policy

I. Preamble. The Federal Trade Commission ("FTC") has instituted a rule (the "Rule"[1]), whereby all creditors, as defined in the Rule, must implement a written identity theft prevention program to detect, prevent and mitigate identity theft in connection with i) the opening of an account or ii) any existing account. The Western Virginia Water Authority (the "Authority") is a creditor for purposes of the Rule.

II. Identity Theft Policy. It shall be the policy of the Authority that employees of the Authority shall take certain steps to comply with the Rule as hereinafter defined, which steps together shall constitute the Authority's Identity Theft Policy (the "Policy" or "Program"). Also contained in this Policy are the Authority procedures for compliance with the Virginia breach of personal information notification statute.

A. Opening New Customer Accounts. Whenever any new customer applies to the Authority for water and/or sewer service, the Authority shall require the applicant to submit certain information, including but not limited to, the applicant's name, the address for which service is requested, and the applicant's social security number.

Upon the securing of this information, the Authority shall run a check on these three information fields against the Authority's current database in order to see if any of the fields are duplicates.

In the event that any duplicate names, addresses or social security numbers show up on the Authority's current database, the Authority shall identify the duplicates as "Red Flags" and shall then use due diligence in order to determine whether any identify theft is being attempted or has occurred.

Such due diligence shall include an attempt to verify the validity of any new customer information that is submitted and that has been identified as a Red Flag, as well an attempt to verify the validity of the information on the existing database that comprises the Red Flag. If in the Authority's opinion invalid information has been submitted or exists on the system, the Authority shall notify the customer(s) in question. As appropriate, the Authority may also take such other steps including:

1) monitoring of the new and existing accounts;
2) not opening the new account;
3) closing the existing account;
4) notifying law enforcement officials; or
5) making a determination that no response is warranted under the particular circumstances.

[1] 16 CFR Part 681

B. Existing Customer Accounts. The Authority shall regularly monitor existing customer accounts, authenticating customers where necessary, monitoring transactions and any suspicious account activity and verifying the validity of any change of address requests or other account change requests. In addition, where appropriate, the Authority may also take any of the steps listed in II.A.2 and II.A.4.-7 above.

C. Ongoing Administration. The Authority shall take such steps so as to periodically update its procedures for detecting Red Flags and potential identity theft, taking into account factors such as the Authority's experiences with identity theft and changes in the methods to identify and mitigate identity theft. As well, the Authority Board of Directors or some committee of the same shall have oversight over the Program and shall be provided reports by Authority staff generated in conjunction with the running of the Program. In addition, the Authority shall update this Policy from time to time as needed, and in order to maintain compliance with the Rule, as contained in 16 CFR Part 681.

D. Virginia Breach of Personal Information Notification Statute. The Authority shall take such steps as are necessary in order to stay in compliance with the Virginia Breach of Personal Information Notification Statute, Virginia Code Section 18.2-186.6 (the "Statute"). The Statute requires the Authority to report any unauthorized breaches of its customer database or other systems housing personal information of its customers. The report must be made to both the Office of the Attorney General and to any affected customer whose personal information has been, or is reasonably believed to have been accessed and acquired by an unauthorized person. The Statute specifies the type of notice that is acceptable. Acceptable notice includes:

1) written notice to the last known postal address in the records of the customer or business;
2) telephone notice;
3) electronic notice; or
4) substitute notice, in specific instances under the Statute.

The contents of, and description to be included in the notice are specified in the Statute. The Authority shall update this Policy from time to time in order to maintain compliance with the Statute.

PART 1
DEFINITIONS

1. For purposes of this Policy, the term *"Account"* shall mean a personal or business utility account with Western Virginia Water Authority.

2. For purposes of this Policy, the term *"Identity Theft"* shall mean a fraud committed or attempted using the identifying information of another person without their permission or authority.

3. For purposes of this Policy, the term *"Red Flag"* shall mean a pattern, practice, or specific activity that indicates the possible existence of identity theft. Part 2 provides a specific description of which Red Flags are applicable to this policy.

4. For purposes of this Policy, the term "*Duplicate information*" shall mean the same name, birth date, and ID provided is found against one or more addresses in our current records.

5. For purposes of this Policy, the term "*Mismatched information*" shall mean the ID provided is found in our records but the name provided does not match the name associated with our records and vice versa; or date of birth provided does not match the date of birth associated with our records.

6. For purposes of this Policy, the term "*Key account information*" shall mean the data elements required in order to open an account (the full name, date of birth, service address, and ID number).

7. For purposes of this Policy, the term "*ACCV Code*" shall mean the access violation code and associated information used when documenting an account for a possible red flag. The information entered in the miscellaneous note will be name of person calling; phone number from caller identification, when available; and nature of information attempting to acquire.

PART 2
IDENTIFICATION OF RELEVANT RED FLAGS

The Western Virginia Water Authority adheres to the following procedure when opening a new account for utility billing or credit financing for a new connections, when accessing account information, and when updating account information on existing accounts in order to determine potential identity theft. This procedure shall be followed when interacting with customers in person and on the telephone. In addition, cashiers will identify potential identity theft when processing check payments.

The following events/occurrences are considered "Red Flags" for purposes of this policy:

A. The presentation of suspicious documents, such as:

1. Documents provided for identification which appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

3. A lease appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

B. Providing suspicious personal identifying information:

1. The Identification Number provided is the same as that submitted by another customer.

2. The person attempting to open or access account information fails to provide all required personal identifying information.

3. Personal identifying information provided is not consistent with personal identifying information that is on file with Western Virginia Water Authority.

C. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with accounts serviced by the Western Virginia Water Authority.

PART 3
DETECTION, PREVENTION AND MITIGATION

The three processes within the Authority which may result in the detection of identity theft:

- When an account is opened
- When an account is accessed
- When payments are made on the account.

1. Opening an account

   Detection
   In order for a customer to open a new account, they must provide at least the following information/documentation:

   a. Full Name;

   b. Date of birth (individual);

   c. Service Address, and;

   d. Identification number, which shall be: (i) For a U.S. citizen, a social security number; or (ii) For a non-U.S. citizen, one or more of the following: a social security number; passport number and country of issuance, I-94 form with refugee number, or a valid driver's license number;

   The following optional information may be provided and, if provided, will be validated:

   e. Additional Name to have access to the account;

   f. Social Security number of additional name to have access to the account;

   g. Date of Birth (individual) of additional name to have access to the account;

   h. A valid lease may be required for rented properties.

   Prevention

   If the customer wanting to open a new account provides documents for identification or a signed lease or signed purchase documents that appear to be altered or forged, the account will not be opened. Also, if the photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification, the account will not be opened.

   Once the *key account elements* are received, the customer service representative will check for *duplicate* or *mismatched* information against existing customer information records. If there is no *duplicate* or *mismatch*, the account will be opened. If there is duplication, the customer service representative will check whether the information is associated with an inactive account in which case the account will be opened. If the information is associated with an active account, the customer service representative will follow up with the customer to see if they want the existing account closed as

well as opening the new account.

Mitigation
When *duplicate information* is found **and** the person's response is that they have not had service with the Authority, or when there is *mismatched information* the customer service representative will ask them to come to our offices with their *key account information* as well as a signed lease or signed purchase documents. The existing account(s) will be investigated and, if determined to be subject to possible identity theft, the "*ACCV Code*" information must be added on the existing account(s).

- If the person does not come in within 3 business days, and there is an active account at the service address in question, a customer service representative will contact that customer to warn of a potential identity theft. A decision will be also be made as to what additional actions are needed, including a determination if it is necessary to contact law enforcement.
- If the person does come in and present their *key account information* and a signed lease or signed purchase document, the existing customer will be contacted to verify their *key account information*. If our records on file are incorrect, we will make the necessary correction(s), otherwise the existing account will be reported for identity theft.

2. Account Access

Detection
In order for a customer to access an account, they must provide at least the following information/documentation:

a. Full name (must also be listed on account if not the primary account holder to access the account);

b. Social security number;

c. Full Name of the primary account holder (if different from 2a);

d. Service Address;

e. Date of birth (individual);

f. Password (when required).

Prevention
If the customer service representative finds a mismatch on any of the information given to access the account, no account information will be given, nor will any changes be made on the account.

Mitigation
An access violation note, "*ACCV Code*," will be entered on the account documenting the access attempt. The information entered on the note will include the name of

person calling; phone number from caller identification, when available; and nature of information attempting to acquire. The account will also be monitored for 60 days and reviewed to determine if any additional action is necessary.

3. Payment Processing

   Detection
   When payments are processed on an account in the collections department, the cashier will review the name and address on the check to verify that the name and address match the existing account information. If the name or address does not match the account name or address, or a name that has been given access to the account, the account holder will be contacted by a customer service representative within 3 days to ensure that no identity theft has occurred.

   Prevention
   If payments are being made on an account for a deceased person and the estate has been settled, or if the person making payments does not place the account in their own name, the account will be reviewed to determine the necessity of closing the account.

   Mitigation
   If customer is not aware of someone else making payments on the account, a red flag will be noted and the account will be reviewed to determine the necessity of closing the account, as well as making a decision as to collecting the debt owed on the account.

A report will be run monthly listing accounts noted with the "*ACCV Code*" and the accounts will be reviewed again to determine whether any additional action is required.

For any account holder of an account for which the "*key account information*" is not already on file at Western Virginia Water Authority, the customer will be contacted within two weeks after discovering the missing information to obtain the necessary information. Updates will also take place during customer service contact with the customer.

PART 4
PROGRAM UPDATES

Western Virginia Water Authority is committed to maintaining an Identity Theft Prevention Policy that is current with the ever-changing crime of identity theft. To that end, Western Virginia Water Authority will reassess this policy on a periodic (annual) basis. In reassessing this policy, Western Virginia Water Authority will add/delete Red Flags in Part 2, as necessary, to reflect changes in risks to customers or to the safety and soundness of Western Virginia Water Authority from identity theft. The determination to make changes to this policy will be within the discretion of Western Virginia Water Authority Management, but after careful consideration of the following:

1. Western Virginia Water Authority's past experience(s) with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent, and mitigate identity theft;

4. Changes in the types of accounts that Western Virginia Water Authority offers; and

5. Changes in the business arrangements of Western Virginia Water Authority, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.