

MONROE COUNTY WATER AUTHORITY
IDENTITY THEFT PREVENTION POLICY
(ADOPTED MARCH 2009; AMENDED MAY 2009)

Section 41.90 of Title 12 of the Code of Federal Regulations (the “Regulations”) requires every “utility” that offers or maintains a “covered account” to develop and maintain a written identity theft prevention policy to detect, prevent and mitigate identity theft. The purpose of this Policy is to comply with the Regulations, as well as any similar requirements put forth by the State of New York. Accordingly, this Policy will only apply to customer accounts held primarily for residential purposes.

ARTICLE I.
ASSESSMENT OF EXISTING BUSINESS PRACTICES

Monroe County Water Authority (the “Authority”) will periodically assess its existing customer service business practices in order to identify areas of potential risk for identity theft. In its initial examination, the Authority has identified the following business practices that could raise “red flags” indicating the potential for identity theft:

1. Methods of Opening New Accounts. A customer can open a new account either over the telephone or in-person, in each case with a live customer service representative. The Authority will require the customer to complete and sign a New Service Application Letter or New Customer Application Letter which will require, but is not limited to, providing the following personal identifying information:

- Name;
- Property Address; and
- Telephone Number.

The Authority will issue a four-digit Customer Code to each customer account upon activating water service.

2. Methods of Transferring an Existing Account. Upon a sale of real property, an existing account holder (“Existing Account Holder”) can transfer its account to a new customer (“New Account Holder”) either over the telephone or in-person, in each case with a live customer service representative. The Authority will require the new customer to complete and sign a New Customer Application Letter which will require, but is not limited to, providing the following personal identifying information in order to transfer an existing account:

- Name of Existing Account Holder;
- Account Number;
- Customer Code of Existing Account Holder;
- Name of the Attorney of Existing Account Holder;

- Telephone Number of Existing Account Holder;
- Property Address;
- Name of New Account Holder;
- Telephone Number of New Account Holder;
- Name of the Attorney of the New Account Holder;
- Date of Closing on the Sale of the Serviced Property; and
- Date of Existing Account will be Transferred to New Account Holder.

However, in the event that the property transfer is the result of a foreclosure sale, then the Authority may require the following information in lieu of the specified Existing Account Holder information:

- Evidence provided by the New Account Holder that the New Account Holder is purchasing the subject property through a foreclosure sale; or
- Verification by a customer service representative that the Authority's records indicate that the subject property has been foreclosed upon.

3. Methods of Accessing Existing Account Information. A customer can access their account information via telephone or in-person, in each case with a live customer service representative, or through the Authority's website.

Telephone or In-person Access. The Authority requires the following Existing Account Holder information for the customer to gain such access:

- Name;
- Account Number;
- Customer Code;
- Telephone Number; and
- Property Address.

A customer may also permit a third party to access their Existing Account Information by (i) contacting the Authority via telephone or in-person, (ii) providing the requisite Existing Account Holder information to gain access, (iii) requesting that the Authority grant the named third party access and (iv) specifying the extent of such access.

Website Access. A customer must enter the following Existing Account Holder information in order to gain access:

- Account Number; and
- Property Address.

The following Existing Account Holder information is available through the Authority's website:

- Name;
- Billing Information;
- Account Balance;
- Current Payment Information;
- Payment History;
- Meter Read Information; and
- Consumption History.

4. Methods of Terminating Water Service. A customer can terminate water service either over the telephone or in-person, in each case with a live customer service representative. The Authority requires the following Existing Account Holder information in order to terminate water service:

- Name;
- Account Number;
- Customer Code;
- Telephone Number; and
- Property Address.

5. Automatic Bill Payment. A customer may set up automatic bill payment by submitting a voided blank check and a signed Authorization Form that includes the following personal identifying information:

- Name;
- Account Number;
- Checking Account Number;
- Property Address;
- Telephone Number; and
- Email Address (if any).

If any of the above information leads to a case of identity theft, the Authority shall perform the corrective actions set forth hereinafter.

ARTICLE II. IDENTIFICATION OF RED FLAGS

The Authority has identified the following circumstances as potential indicators of identity theft (collectively, the "Red Flags"):

1. Identifying information provided to establish or transfer an account, or terminate water service appears suspicious or is not consistent with readily accessible information on file with the Authority, such as information in customer service records.
2. Information provided is associated with known fraudulent activity (*e.g.*, name, address and/or phone number on an application is the same as the address provided on a previous fraudulent application).
3. Information provided is of a type commonly known to the Authority as associated with fraudulent activity.
4. Name, address and/or telephone number provided is the same as or substantially the same as the information of an Existing Account Holder.
5. A person attempting to establish or transfer an account fails to provide all required personal identifying information after notification that the required information is incomplete.
6. A person attempts to set up automatic bill payment by providing a voided check and/or Authorization Form with banking information that is inconsistent with the account information on file for the Existing Account Holder.
7. Mail sent to an Existing Account Holder is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the customer's account.
8. The Authority receives written notice from an Existing Account Holder, victim of identity theft, or law enforcement agency that a person has engaged in identity theft by fraudulently opening, accessing, or transferring an account, terminating water service, or by fraudulently setting up automatic bill payment for an account.

**ARTICLE III.
DETECTION OF RED FLAGS**

The following lists the Authority's methods for detecting Red Flags during the routine handling of new and/or existing accounts:

1. Require proper identifying information to open a new account.
2. For requests to access or modify Existing Account Holder information, verify identity by requesting specific personal identifying information.
3. Before transferring an account or terminating water service, verify personal identifying information using records on file.
4. Require customer service representatives to add account notes reflecting any suspicious inquiries or activity on a particular account.
5. For automatic bill payment, verify and cross-check information on voided check and Authorization Form submitted to the Authority with existing customer information for that account.

6. Keep a log of any accounts known to be established, transferred, modified, accessed, closed and/or set up for automatic bill payments as the result of identity theft.

ARTICLE IV. PREVENTION AND MITIGATION

The following lists corrective actions to be taken, as applicable, by customer service representatives if they observe a Red Flag situation.

1. After conferring with a department supervisor, customer service representatives will decline to open a new account. For an existing account, the Authority shall conduct an investigation, including taking any of the following possible actions:

- Continue to monitor the account for evidence of identity theft and contact the customer to discuss possible actions.
- Contact the customer to verify account activity.
- Reopen an existing account with a new account number.
- Terminate water service to an existing account.

2. If the Authority identifies an instance of identity theft associated with an unpaid account, it will not attempt to collect on the account or sell the account to a debt collector.

3. Upon written notification of an incident of identity theft and a request from the Existing Account Holder or victim of identity theft, the Authority will provide any relevant information that lawfully can be disclosed.

4. For all instances of suspected or confirmed identity theft, the Authority will cooperate with local law enforcement and credit reporting agencies and provide them with applicable requested information.

5. The Authority will check references and/or conduct background checks before hiring employees who will have access to customer information.

6. The Authority will require new employees to sign an agreement to follow the Authority's confidentiality and security standards for handling customer information.

7. The Authority will control access to sensitive information by requiring customer service representatives to use "strong" passwords.

8. The Authority will enforce existing policies addressing the appropriate use and protection of laptops, including requiring employees to store laptops in a secure place when not in use.

9. The Authority will train employees to take basic steps to maintain the security, confidentiality and integrity of customer information, including:

- Locking rooms and file cabinets where records are kept.

- Not sharing or openly posting employee passwords in work areas.
- Reporting to designated personnel any suspicious attempts to obtain customer information.

10. The Authority shall regularly remind customer service representatives to keep customer information secure and confidential by posting reminders in areas where customer information is stored, such as the customer service call center.

11. The Authority will develop security and/or technology policies for employees who telecommute.

12. The Authority will impose disciplinary measures for violations of this Policy.

13. In order to prevent terminated employees from accessing customer information, the Authority will immediately deactivate their passwords and user names and take other appropriate measures.

14. The Authority will know where sensitive customer information is stored and store it securely. The Authority will make sure only authorized employees have access to such information and maintain a careful inventory of computers and any other information equipment.

15. The Authority will dispose of customer information in a secure way, using the following disposal methods:

- Hire an outside disposal company or designate a staff member to supervise the disposal of records containing customer information.
- Pulverize or shred papers containing customer information so that the information cannot be read or reconstructed.
- Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs or any other electronic media or hardware containing customer information.

ARTICLE V. PROGRAM ADMINISTRATION

The following lists the ways the Authority will implement and update this Policy.

1. Staff Training. The Authority will provide Red Flags detection and response training to any employee with the ability to access, manage or terminate service to an existing account or open a new account. The Authority will provide similar training to key management personnel, as appropriate. Training information will be updated regularly to reflect the latest developments in detection and response protocols.

2. Program Review and Update. The Authority will review and update this Policy annually to reflect changes in identity theft risks to customers based on factors such as:

- Actual incidents of identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts offered or maintained.
- Changes to the Authority's business, including joint ventures and service provider arrangements.

3. Approval and Adoption. This Policy has been reviewed and approved by the Members of the Authority (the "Board"). The Board hereby assigns to the Director of Finance and Business Services of the Authority responsibility for the oversight, development, implementation and administration of this Policy (the "Red Flag Officer"). The Red Flag Officer will develop an annual report for the Board as described in Section 4 below to assess compliance with this Policy.

4. Annual Reporting. The Red Flag Officer will provide an annual report to the Board that details the Authority's compliance with this Policy and the Regulations. The report will address matters that include:

- Effectiveness of the Authority's policies and procedures in addressing the risk of identity theft, including service provider arrangements;
- Significant incidents involving identity theft and management's response; and
- Recommendations for material changes to this Policy.

5. Service Provider Oversight. The Authority will monitor the actions of service providers engaged to perform activities that involve access to customer information. In particular, the Authority will confirm that such activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The Authority will accomplish the foregoing by requiring that the service provider either have its own acceptable Red Flags policy or that it agrees in writing to follow this Policy.