IDENTITY THEFT PREVENTION PROGRAM

Developed By and For:

Metro Water
Services

Approval of the Initial Program Received From:

Metropolitan Government of
Nashville

On the Following Date:

April 15, 2009

Director, Metro Water Services

Program Reviewed, Updated and Approved on:

Part I. Assessment of Existing Business Practices

Part I of the Identity Theft Prevention Program is used to identify areas of potential risk within Metro Water Services (MWS) standard Customer Service business practices. MWS has selected specific business processes associated with offering or maintaining accounts, or engaging in other activities that could raise "red flags" indicating the potential for identity theft.

A. Metro Water Services provides Customer Service personnel with the ability to request and review a customer's personal identifying information when engaging in any of the following activities:

- ☐ Open new accounts;
- ☐ Obtain new water/sewer permit;
- ☐ Access existing accounts;
- ☐ Modify existing accounts; and/or
- ☐ Close existing accounts.

B. Metro Water Services provides customers with the ability to do one or more of the following actions independent of Customer Service personnel (either through an automated phone system or online), and a customer's personal identifying information is required to complete any of these activities:

- ☐ Open a new account;
- ☐ Access an existing account;
- ☐ Modify an existing account; and/or
- ☐ Close an existing account.

Also, if MWS has identified a past occurrence of identity theft that was linked to a customer's utility account (an unauthorized opening, modifying or closing of an account), then they must perform the actions set forth in the following program.

[redacted] has identified the following items as potential red flag sources of categories that might indicate an instance of identity theft.

- Consumer report includes a fraud or active duty alert, a notice of credit freeze and/or a notice of address discrepancy.
- Consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of the customer, such as a recent and significant increase in the volume of inquiries.
- Documents provided for identification appear to have been altered or forged.
- Photograph, physical description and/or other information on the identification is not consistent with the appearance of the person presenting the identification.
- Information on the identification is not consistent with readily accessible information that is on file with the Utility, such as property tax records or NES.
- Information provided is inconsistent when compared against external information sources (address does not match any address in the consumer report and/or social security number has not been issued or is associated with a deceased person).
- Information provided by the customer is inconsistent with other information provided by the customer (no correlation between SSN range and date of birth).
- Information provided is associated with known fraudulent activity (address and/or phone number on an application is the same as the address provided on a previous fraudulent application).
- Information provided is of a type commonly associated with fraudulent activity (address on an application is fictitious and/or phone number is invalid).
- Social security number, address and/or telephone number provided is the same as or similar to ones provided by another customer.
- Customer fails to provide all required personal identifying information.
- Customer account is used in a manner that is not consistent with established patterns of activity on the account, for example, nonpayment when there is no history of late or missed payments.
- Personal identifying information provided is not consistent with personal identifying information that is on file.
- Customer cannot provide authenticating information beyond that which generally would be available from a consumer report, (driver's license, student id, etc.).
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account
- Utility is notified that the customer is not receiving account statements.
- Utility is notified that it has opened a fraudulent account for a person engaged in identity theft.

Flags as related to possible identity theft during MWS's routine handling of new and/or existing accounts. The following is a list of detection methods that the Utility uses to prevent identity theft.

Require customers to present government-issued identification information to open a new account.

Verification through documents:

Individual – Unexpired government issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license.

Corporation, Partnership, or Trust – Documents showing the existence of the entity, such as certified articles or incorporation, a government issued business license, a partnership agreement, or trust instrument.

Verification through non-documentary methods:

Customer will supply the following information: name, date of birth, social security number, address, phone number.

Contact the customer (in the case of phone or internet setup of new utility accounts)

Verify personal identification information using records on file with the Utility or through a third-party source such as a consumer reporting agency.

When fielding a request to access and/or modify an existing account (such as a change of billing address), verify identity of customer by requesting specific pieces of personal identifying information (identification with the new billing address and/or documentation proving shift of financial liability)

If new banking information is provided for electronic payment of accounts, cross-check ownership of the new banking account with the customer name on the utility account by contacting the appropriate financial institution.

For online or automated phone system access of utility account, require the establishment of security questions during the initial set-up of the account.

personnel if the personnel have observed a Red Flag associated with a new or existing utility account. One of more of the following actions will be taken by the Utility to rectify the situation.

- MWS will not open a new account (after review of the presented identifying information and discussion with department supervisor)

- For an existing account, MWS may discontinue the services associated with that account and/or:

  - Continue to monitor the account for evidence of identity theft and contact the customer to discuss possible actions.
  - Change the passwords, security codes, or other security devices that permit access to an existing account.
  - Reopen an existing account with a new account number.
  - Close an existing account.

- If MWS has identified an instance of identity theft associated with an unpaid account, MWS will not attempt to collect on the account or sell the account to a debt collector.

- MWS will contact the consumer to advise them of the identity theft.

- MWS may determine no response is called for.

- In determining an appropriate response, MWS will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by MWS or a third party or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent MWS or to a fraudulent website.

- If applicable, MWS will provide the consumer reporting agencies with a description of the identity theft event.

- For all instances of suspected or confirmed identity theft, MWS will notify local law enforcement and will provide them with all the relevant details associated with the identity theft event.

This section details the training requirements, annual program review, approval and adoption process and annual reporting requirements that are associated with this Program.

A. Staff Training

Any employee with the ability to open a new account, or access/manage/close an existing account will receive training on identifying and detecting Red Flags. They will also be trained in the appropriate response actions in the event that an instance of identity theft is suspected. Key management personnel in appropriate departments will also receive training on the contents of this Program. As necessary, employees will be re-trained annually if the Program is updated to include new methods of identifying and detecting Red Flags, or if new response actions are implemented.

B. Program Review and Update

MWS will review and update the Program annually to reflect changes in risks to customers from identity theft based on factors such as:

- Previous identify theft experiences at MWS.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that MWS offers or maintains.
- Changes in the business arrangements of MWS, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

C. Program Approval and Adoption

This Program and revisions have been reviewed and approved by MWS' director.

Metro Water Services has assigned the following MWS staff member, Lisa Russell, to be responsible for the oversight, development, implementation and administration of the Program. Annually, the designated staff member will develop the annual report as described in Section D that will address compliance of MWS with this Program. MWS is responsible for reviewing this report and approving material changes to the Program as necessary to address changing identity theft risks.

compliance with the Federal Trade Commission's Red Flags Rule. The report will address matters related to the Program and address several topic areas including:

- Effectiveness of the policies and procedures of MWS in addressing the risk of identity theft in connection with the opening of new accounts and with respect to the management of existing accounts;
- Service provider arrangements;
- Significant incidents involving identity theft and management's response; and,
- Recommendations for material changes to the Program.

E. Service Provider Oversight

Whenever MWS engages a service provider to perform an activity in connection with one or more of the customer accounts, MWS will verify that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To accomplish this, MWS will require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to MWS, or to take appropriate steps to prevent or mitigate identity theft.

following business practices, MWS has elected to do the following:

1. Checking references or doing background checks before hiring employees who will have access to customer information.
2. Asking every new employee to sign an agreement to follow the Utility's confidentiality and security standards for handling customer information.
3. Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
4. Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. Using password-activated screen savers to lock employee computers after a period of inactivity.
5. Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.
6. Training 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;
   Encrypting sensitive customer information when it is transmitted electronically via public networks;
   Referring calls or other requests for customer information to designated ;
   Reporting suspicious attempts to obtain customer information to designated personnel.
7. Regularly reminding all employees of the Utility's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
8. Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
9. Imposing disciplinary measures for security policy violations.
10. Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.
11. Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:

    Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.

physically-secure area.

Where possible, avoid storing sensitive customer data on a computer with an Internet connection.

Maintain secure backup records and keep archived data secure by storing it offline and in a physically-secure area.

Maintain a careful inventory of the Utility's computers and any other equipment on which customer information may be stored.

12. Take steps to ensure the secure transmission of customer information. For example:

When transmitting credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.

If the Utility collects information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.

If the Utility must transmit sensitive data by email over the Internet, be sure to encrypt the data.

13. Dispose of customer information in a secure way and, where applicable, consistent with the FTC's Disposal Rule, www.ftc.gov/os/2004/11/041118disposalfrn.pdf.

MWS currently has a records retention policy in place and a coordinator who updates and maintains the policy.

14. Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:

Check with software vendors regularly to get and install patches that resolve software vulnerabilities;

Use anti-virus and anti-spyware software that updates automatically;

Maintain up-to-date firewalls, particularly if using a broadband Internet connection or allow employees to connect to the network from home or other off-site locations;

Regularly ensure that ports not used for Utility business are closed; and

Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

15. Considering notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:

Notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;

Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;

Notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm; and

Check to see if breach notification is required under applicable state law.