Identity Theft Prevention Program

For the

Washington Township Municipal Authority

11102 Buchanan Trail East

Waynesboro, PA 17268

May 1, 2009

WTMA Identity Theft Prevention Program

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, ensure existing accounts were not opened using false information, and to respond to such events.

For the purposes of this policy, **Personal Information** includes information such as driver's license information and Social Security numbers. It does not include information such as name, address and phone number.

Contact Information:

The Senior Management Person responsible for this program is the Manager:

Name: Sean McFarland

Title: Manager

Phone number: 717-762-3108 x104

The Governing Body Members of the Utility are:

1. Fred Eisenhart, Chairman
2. Stewart McCleaf, Vice Chairman
3. Lori Frantz, Secretary/Treasurer
4. Elaine Gladhill, Asst. Secretary/Treasurer
5. John E. N. Blair, Member

Risk Assessment

The Washington Township Municipal Authority has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information the Authority was able to identify red flags that were appropriate to prevent identity theft.

- ❑ New accounts opened In Person
- ❑ New accounts opened via Telephone
- ❑ Account information accessed In Person
- ❑ Account information accessed via Telephone (Person)

Detection (Red Flags)

The Washington Township Municipal Authority adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- ❑ Identification documents appear to be altered
- ❑ Photo and physical description do not match appearance of applicant
- ❑ Other information is inconsistent with information provided by applicant
- ❑ Other information provided by applicant is inconsistent with information on file.
- ❑ Personal information provided by applicant does not match other sources of information
- ❑ Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- ❑ Customer fails to provide all information requested
- ❑ Personal information provided is inconsistent with information on file for a customer
- ❑ Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- ❑ Identity theft is reported or discovered

Response

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the Manager

- ❑ Ask applicant for additional documentation
- ❑ Notify internal manager: Any Authority employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the Manager.

- ❑ Notify law enforcement: The Authority will notify the Washington Township Police of any attempted or actual identity theft.
- ❑ Do not open the account
- ❑ Close the account

Personal Information Security Procedures

The Washington Township Municipal Authority may ask for identification to verify the identity of an individual upon opening or closing an account, making changes to an account (e.g. changing a billing to a tenant), or other reasonable purposes. Any proof of identity will be destroyed and will not be maintained by the Authority.

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the Washington Township Municipal Authority Board of Directors. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Signatures:

1. _____ Date 4-21-09
2. _____ Date 4-21-09
3. Lori Frantz _____ Date 4/21/09
4. Elaine A Gladhill _____ Date 4/21/09
5. John F. X. Blair _____ Date 4/21/09

A report will be prepared annually and submitted to the Board of Directors to include matters related to the program, the effectiveness of the policies and procedures, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

Appendix A
Other Security Procedures

The following is a list of other security procedures the Authority will implement to protect personal data (including that of Authority staff members).

1. Paper documents, files, and electronic media containing personal information will be stored in a secure file cabinet..
2. Only specially identified employees with a legitimate need will have access to the file cabinet.
3. Files containing personally identifiable information are kept in a secure file cabinet except when an employee is working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas
6. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
7. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
8. Computer passwords will be required.
9. The computer network will have a firewall where your network connects to the Internet.
10. Check references or do background checks before hiring employees who will have access to sensitive data.
11. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
12. Procedures exist for making sure that workers who leave your employ no longer have access to sensitive information.
13. Employees will be alert to attempts at phone phishing.
14. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
15. Paper records containing personal information will be shredded before being placed into the trash.

16. Outside contractors access to sensitive information should be carefully controlled and locks and passwords changed if relationships change.

17. Change locks and passwords with employee turnovers as needed.