RESOLUTION TO PROVIDE AN IDENTITY THEFT PREVENTION PROGRAM TO COMPLY WITH FEDERAL REGULATIONS
#09-32

Identity Theft Prevention Program

For

Battle Ground Sewage Utilities

100 College Street
Battle Ground, Indiana 47920

April 13, 2009

Battle Ground Utilities Identity Theft Prevention Program Pursuant to federal law the Federal Trade Commission (FTC) adopted Identity Theft Rules requiring the creation of certain policies relating to the use of consumer reports, address discrepancies and the detection and prevention of identity theft.

This Plan is intended to comply with the FTC by identifying red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

Contact Information:

The Person responsible for this plan is:

Clerk-Treasurer 765-567-2603

The Governing Body Members of the Utility are:
Battle Ground Sewage Department

1. Utility Superintendent
2. Council President

Risk Assessment

Battle Ground Utilities 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 utility was able to identify red flags that were appropriate to prevent identity theft:

1. New accounts opened In Person
2. Account information accessed In Person
3. Account information accessed via Telephone (Person)

Detection (Red Flags):

Battle Ground Utilities 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:

1. Photo and physical description do not match appearance of applicant.
2. Other information is inconsistent with information provided by applicant.
3. Other information provided by applicant is inconsistent with information on file.
4. Personal information provided by applicant does not match other sources of information.
5. Information provided is associated with known fraudulent activity. (address or phone number provide is same as that of a fraudulent application)
6. Information commonly associated with fraudulent activity is provided by applicant. (Address that is a mail drop, non-working phone number or associated with answering service/pager)
7. Phone number same as other customer at utility.
8. Customer fails to provide all information requested.
9. Personal information provided is inconsistent with information on file for a customer.
10. 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 superintendent.

1. Ask applicant for additional documentation
2. Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the Clerk-Treasurer.
3. Notify law enforcement: The utility will notify the Battle Ground Police Department at 765-567-2223 of any attempted or actual identity theft.
4. Do not open the account.
5. Close the account.
6. Do not attempt to collect against the account, but notify authorities.

Personal Information Security Procedures Battle Ground Utilities adopts the following security procedures:

1. All new accounts must be opened in person at the Battle Ground Town Hall.
2. Paper documents, files and electronic media containing secure information will be stored in locked file cabinets.
3. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
4. Employees will store files when leaving their work areas.
5. Employees will log off their computer when leaving their work areas.
6. Access to sensitive information will be controlled using passwords. Employees will choose passwords with a mix of letters, numbers and characters. User name and passwords will be different. Passwords will be changed at least monthly.
7. Password will not be shared or posted near workstations.
8. Anti-virus and anti-spy ware programs will be run on individual computers and on servers regularly.
9. When installing new software, vendor-supplied default passwords will be changed.
10. The computer network will have a firewall where the network connects to the Internet.
11. Access to a customer's personal identify information will be limited to employees with a "need to know".
12. Paper records will be shredded before being placed into the trash.

Periodic Updating of Program

Battle Ground Utilities will monitor identity theft schemes reported on the internet, and in the mainstream media such as radio and television, in order to continually reevaluate the appropriateness and adequacy of its Theft Prevention Program.

Identity Theft Prevention Program Review and Approval This plan has been reviewed and adopted by the Battle Ground Town Council. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Sigatures:

Becky Holladay
Council President

A report will be prepared and submitted to the superintendent or governing body of any changes that are needed to improve the effectiveness or any oversights of our policies as needed.