Identity Theft Prevention Program

For

IMPROVE WATER ASSOCIATION

227 SAWMILL RD.
SANDY HOOK, MS. 39478

AMENDED: AUGUST 14, 2012

Improve Water Association
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, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

Contact Information:

The Senior Management Person responsible for this program is:
Name: __Donald Thomas__
Title: __President_______
Phone number: __(601)810-9804 cell__

The Governing Body Members of the Utility are:
Board Members

1.__Donald Thomas___________President

2.__Marshall Pittman Jr. Vice-President

3.__ Versie Dee Lee______ _Secretary

4.__Lester Thomas___________Treasurer

5.__O. L. Hughes_______Board Member

Risk Assessment

The Improve Water Association 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. Add or delete items as applicable:

- ❑ New accounts opened In Person
- ❑ New accounts opened via Telephone
- ❑ Account information accessed In Person
- ❑ Account information accessed via Telephone (Person)
- ❑ Account information is accessed via Web Site
- ❑ Identity theft occurred in the past from someone falsely opening a utility account

---

Detection (Red Flags):

The Improve Water Association 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.

- ❑ Fraud or active duty alerts included with consumer reports
- ❑ Notice of credit freeze provided by consumer reporting agency
- ❑ Notice of address discrepancy provided by consumer reporting agency
- ❑ Inconsistent activity patterns indicated by consumer report such as:
    - Recent and significant increase in volume of inquiries
    - Unusual number of recent credit applications
    - A material change in use of credit
    - Accounts closed for cause or abuse
- ❑ 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.
- ❑ Application appears altered or destroyed and reassembled
- ❑ Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
- ❑ Lack of correlation between the SS# range and date of birth
- ❑ Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- ❑ Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- ❑ SS#, address, or telephone # is the same as that of other customer at utility
- ❑ 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 senior management official.

- □ Ask applicant for additional documentation
- □ Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify _Donald Thomas
- □ Notify law enforcement: The utility will notify__Walthall County Sherriff Dept._____ of any attempted or actual identity theft.
- □ Do not open the account
- □ Close the account
- □ Do not attempt to collect against the account but notify authorities

Personal Information Security Procedures:

The Improve Water Association adopts the following security procedures (select appropriate procedures from Appendix A and add other procedures as appropriate).

1. 1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room
2. Employees log off their computers when leaving their work areas
3. No visitor will be given any entry codes or allowed unescorted access to the office
4. Access to sensitive information will be controlled using “strong” passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.
5. Passwords will not be shared or posted near workstations.
6. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
7. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
8. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
9. Computer passwords will be required.
10. User names and passwords will be different.
11. The use of laptops is restricted to those employees who need them to perform their jobs.
12. Laptops are stored in a secure place.

13. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.

14. If a laptop must be left in a vehicle, it is locked in a trunk.

15. The computer network will have a firewall where your network connects to the Internet.

16. Any wireless network in use is secured.

17. Check references or do background checks before hiring employees who will have access to sensitive data.

18. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.

19. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.

20. Employees will be alert to attempts at phone phishing.

21. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.

22. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.

23. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.

24. Paper records will be shredded before being placed into the trash.

25. Paper shredders will be available at each desk in the office, next to the photocopier, and at the home of any employee doing work at home.

Identity Theft Prevention Program Review and Approval

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

Signatures:

1.____ Date________________

Donald Thomas President of the Board

2.____ Date________________

Marshall Pittman Vice-President of the Board

3.____ Date________________

Versie Dee Lee Secretary of the Board

4.____ Date________________

Lester Thomas Treasure of the Board

5.____ Date________________

Kevin Breland Member of the Board

A report will be prepared annually and submitted to the above named governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.