Identity Theft Prevention Program

For

Gran Mutual Water Company

P. O. Box 1495

Chico, California, 95927-1495

November, 20, 2008

Gran Mutual Water Company

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: Marilyn Everett
Title: Secretary/Treasurer
Phone number: 530 342-6137

The Governing Body Members of the Utility are:
Board Members

1. Randy Hill
2. Marilyn Everett
3. Dan Boone
4. Garey Weibel
5. Bill Beckett

Web site: www.granmutual.org

Risk Assessment

The Gran Mutual Water Company 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.

Member accounts are limited to 106 connections which are identified by parcel number. The name, mailing address, phone number and e-mail address are collected on file for billing and emergency notice procedures. The Gran Mutual Water Company does not have credit or social security number information in the files.

Gran Mutual allows:

- New accounts opened when notification comes from the Escrow regarding the change in ownership of one of the memberships. Title company information and any additional details provided by the new member make up all the information in Gran Mutual files.

Detection (Red Flags):

The Gran Mutual Water Company 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.
- Application appears altered or destroyed and reassembled.
- 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. Add or delete items as applicable:

- ❑ 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 Marilyn Everett 530 342-6137.
- ❑ Do not open the account.

Personal Information Security Procedures:

The Gran Mutual Water Company adopts the following security procedures:

1. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
2. Employees store files when leaving their work areas.
3. Employees log off their computers when leaving their work areas.
4. Employees store files when leaving their work areas.
5. Employees log off their computers when leaving their work areas.
6. No visitor will be given any entry codes or allowed unescorted access to the office.
7. Passwords will not be shared or posted near workstations.
8. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
9. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
10. When sensitive data is received or transmitted, secure connections will be used.
11. Check references or do background checks before hiring employees who will have access to sensitive data.

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

13. Access to customer's personal identify information is limited to employees with a "need to know."

14. Implement a regular schedule of employee training.

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

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. Randy Hill Date 11/20/2008
2. William D. Moore Date 11/20/2008
3. Darrell Weitzel Date 11/20/2008
4. Marilyn Rivera Date 11/20/2008
5. W. Brent Date 11/20/2008

A report will be prepared annually and submitted to the above named senior management or 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.