PINOS ALTOS MUTUAL DOMESTIC WATER CONSUMERS ASSOCIATION

IDENTITY THEFT PREVENTION PROGRAM ("ITPP")

INTRODUCTION

Pursuant to federal law, the Federal Trade Commission adopted Identity Theft Rules requiring the creation of certain policies relating to the use of consumer reports, address discrepancy and the detection, prevention and mitigation of identity theft. The Federal Trade Commission regulations adopted as 16 CFR § 681.2 require creditors, as defined by 15 U.S.C.§ 681(a)(5) to adopt red flag policies to prevent and mitigate identity theft with respect to covered accounts. 15 U.S.C. § 1681a(r)(5) cites 15 U.S.C § 1691a, which defines a creditor as a person that extends, renews or continues credit, and defines "credit" in part as the right to purchase property or services and defer payment therefore. The Federal Trade Commission regulations include utility companies in the definition of creditor. The Pinos Altos Mutual Domestic Water Consumers Association ("PAMDWCA") is a creditor with respect to 16 CFR § 681.2 by virtue of providing utility services or by otherwise accepting payment for municipal services in arrears.

The Federal Trade Commission regulations define "covered account" in part as an account that a creditor provides for personal, family or household purposes that is designed to allow multiple payments or transactions and specifies that a utility account is a covered account. The Federal Trade Commission regulations require each creditor to adopt an Identity Theft Prevention Program (ITPP), which will use red flags to detect, prevent and mitigate identity theft related to information used in covered accounts. The PAMDWCA provides water services for which payment is made after the product is consumed or the service has otherwise been provided which by virtue of being utility accounts are covered accounts. The PAMDWCA residential/commercial Association Member accounts for water services for which payment is made after the product is consumed or the service has otherwise been provided are covered accounts by virtue of being primarily for household purposes and allowing for multiple payments or transactions.

IDENTITY THEFT PREVENTION PROGRAM

1. Purpose.

The purpose of this Program is to comply with 16 CFR § 681.2 in order to attempt to detect, prevent and mitigate identity theft by identifying and detecting identity theft red flags and by responding to such red flags in a manner that will help prevent identity theft.

2. Definitions.

For the purposes of this Program, the definitions found in Appendix A shall apply.

3. Findings.

1) The PAMDWCA is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.
2) Covered accounts offered to Association Members for the provision of PAMDWCA services include residential and commercial water accounts.
3) The PAMDWCA has no known prior experience with identity theft related to covered accounts.
4) The processes of opening a new covered account, restoring an existing covered account, and making payments on such accounts have been identified as potential processes in which identity theft could occur.
5) The PAMDWCA limits access to personal identifying information to the Bookkeeper who is responsible for or otherwise involved in opening or restoring covered accounts or accepting payment for use of a covered account. All written applications (sample included as Appendix B) associated with the covered accounts are maintained in the locked storage locker. Information provided in the application is entered directly into the PAMDWCA's computer system and is accessible only to those employees in the Bookkeeping department and to the PAMDWCA's Board of Directors.
6) The PAMDWCA has determined that there is a low risk of identity theft occurring in the following ways, if any:
   a. Use by an applicant of another person's personal identifying information to establish a new covered account;
   b. Use of a previous Association Member's personal identifying information by another person in an effort to have service restored in the previous Association Member's name;
   c. Use of another person's credit card, bank account, or other method of payment by a Association Member to pay such Association Member's covered account or accounts;
   d. Use by a Association Member desiring to restore such Association Member's covered account of another person's credit card, bank account, or other method of payment; and
   e. Use by a third party of a Association Member's personal identifying information obtained by overhearing conversations between the PAMDWCA and the Association Member during the Association Member's application for service process.

PROCEDURES

4. Process of Establishing a Covered Account.

A. As a precondition to opening a covered account in the PAMDWCA, each applicant shall provide the PAMDWCA with personal identifying information of the Association

Member, which shall be in the form of a valid state Deed of Trust for proof of ownership and all fees as per the Operations Policy.

B. Each account shall be assigned an account number, which the bookkeeper assigns.

C. An applicant's personal identifying information shall be entered directly into the PAMDWCA's computer system and all written applications shall be placed in the storage locker.

D. PAMDWCA employees responsible for opening new accounts shall take reasonable precautions to insure that third parties are not attempting to view personal identifying information on a written application as it is being completed by the applicant.

E. The PAMDWCA does not now allow Association Members to pay billing statements online. Should the PAMDWCA begin allowing online payments, additional precautions will be put in place to address the issue at that time.

5. Access to Covered Account Information.

A. Access to Association Member accounts shall be password protected and shall be limited to authorized PAMDWCA Finance personnel.

B. Passwords shall be changed as deemed necessary.

C. Any unauthorized access to or other breach of Association Member accounts is to be reported immediately to the Board of Directors and the password shall be changed immediately.

D. Personal identifying information included in Association Member accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Bookkeeper and Board of Directors, and if the situation warrants, the Association attorney.

6. Credit Card Payments.

A. At the present time, the PAMDWCA does not allow payments through the Internet. If in the future such payments are allowed, appropriate guidelines will be put into place to certify that an adequate identity theft prevention program is in place that is applicable to such payments.

7. Sources and Types of Red Flags.

All employees responsible for or involved in the process of opening a covered account, restoring a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

A. *Alerts from consumer reporting agencies, fraud detection agencies or service providers (if a consumer credit report is used).* Examples of alerts include, but are not limited to:
   1) A fraud or active duty alert that is included with a consumer report;
   2) A notice of credit freeze in response to a request for a consumer report;
   3) A notice of address discrepancy provided by a consumer reporting agency;
   4) Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or Association Member, such as:
      a. A recent and significant increase in the volume of inquiries;
      b. An unusual number of recently established credit relationships;
      c. A material change in the use of credit, especially with respect to recently established credit relationships; or
      d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. *Suspicious documents*. Examples of suspicious documents include:
   1) Documents provided for identification that appear to be altered or forged;
   2) Identification on which the information is inconsistent with the information provided by the applicant or Association Member;
   3) Identification on which the information is inconsistent with readily accessible information that is on file with the PAMDWCA;
   4) An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

C. *Suspicious personal identification, such as suspicious address change.* Examples of suspicious identifying information include:
   1) Personal identifying information that is inconsistent with external information sources used by the PAMDWCA. For example:
      a. The address does not match any address in the consumer report (if used by the PAMDWCA); or
      b. The social security number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File (if used by the PAMDWCA).
   2) Personal identifying information or a phone number or address, is associated with known fraudulent application or activities as indicated by internal or third-party sources used by the PAMDWCA.
   3) Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.
   4) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of applicants or Association Members.
   5) The applicant or Association Member fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
   6) Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.

7) The applicant or Association Member cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. *Unusual use of or suspicious activity relating to a covered account.* Examples of suspicious activity include:
   1) An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
      a. Nonpayment when there is no history of late or missed payments;
      b. A material change in the water usage.
   2) Mail sent to the Association Member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Association Member's account.
   3) The PAMDWCA is notified that the Association Member is not receiving paper account billings.
   4) The PAMDWCA is notified of unauthorized charges or transactions in connection with a Association Member's account.
   5) The PAMDWCA is notified by a Association Member, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

E. *Notice from Association Members, law enforcement, victims or other reliable sources regarding possible identity theft or publishing relating to covered accounts.*

8. Prevention and Mitigation of Identity Theft.

A. Restoring an Existing Covered Account or Accepting Payment: In the event that any PAMDWCA employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Board of Directors or relevant designee. If the employee at his or her own discretion deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall also convey this information to the Board of Directors or relevant designee, who may at his or her own discretion determine that no further action is necessary. If the Board of Directors, at his or her own discretion determines that further action is necessary, a PAMDWCA employee shall perform one or more of the following responses, as determined to be appropriate by the Board of Directors:
   1) Contact the Association Member;
   2) Make the following changes to the account if, after contacting the Association Member, it is apparent that someone other than the Association Member has accessed the Association Member's covered account:
      a. Change any account numbers, passwords, security codes, or other security devices that permit access to an account; or
      b. Close the account;
   3) Cease attempts to collect additional charges from the Association Member and decline to sell the Association Member's account to a debt collector in the event

that the Association Member's account has been accessed without authorization and such access has caused additional charges to accrue;

4) Notify a debt collector within three (3) business days of the discovery of likely or probable identity theft relating to a Association Member account that has been sold to such debt collector in the event that a Association Member's account that has been sold to such debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;
5) Notify law enforcement, in the event that someone other than the Association Member has accessed the Association Member's account causing additional charges to accrue or accessing personal identifying information; or
6) Take other appropriate action to prevent or mitigate identity theft.

B. Opening a New Covered Account: In the event that any PAMDWCA employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect to an application for a new account, such employee shall use his or her discretion to determine whether such red flags or combination of red flags suggests that identity theft or attempted identity theft is likely or probable. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Board of Directors or relevant designee. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall also convey this information to the Board of Directors or relevant designee, who may, in his or her discretion, determine that no further action is necessary. If the Board of Directors, in his or her discretion, determines that further action is necessary, an appointed PAMDWCA employee shall perform one or more of the following responses, as determined to be appropriate by the Board of Directors:

1) Request additional identifying information from the applicant;
2) Deny the application for the new account;
3) Notify law enforcement of possible identity theft; or
4) Take other appropriate action to prevent or mitigate identity theft.

9. Updating the Program.

The Board of Directors shall annually review and, as deemed necessary, update the Identity Theft Prevention Program (ITPP) along with any relevant red flags in order to reflect changes in risks to Association Members or to the safety and soundness of the PAMDWCA and its covered accounts from identity theft. In doing so, the Board of Directors shall consider the following factors and exercise its discretion in amending the program:

1) The PAMDWCA's experiences with identity theft;
2) Updates in methods of identity theft;
3) Updates in customary methods used to detect, prevent, and mitigate identity theft;
4) Updates in the types of accounts that the PAMDWCA offers or maintains; and
5) Updates in service provider arrangements.

10. Program Administration.

A. In accordance with specified guidelines, the PAMDWCA governing body has designated an Oversight Committee composed of the Treasurer and the Bookkeeper to ensure the

Program's regulatory compliance. The Oversight Committee is responsible for, but not limited to:

1) The development and implementation of the Program.
2) Ensuring compliance with all Program requirements as stated in this policy;
3) Conduct a periodic review of all incidents involving one or more red flag events every six months (on or about May 15 and November 15 of each year).
4) At least annually, review staff reports regarding compliance with this policy and Red Flag events that occurred during the reporting period.
5) At least annually, address and agree on any changes that may need to be made to the Program and submit these annually for consideration.

B. The Board of Directors is responsible for reviewing reports (prepared at least bi-annually) regarding compliance with red flag requirements and with recommending material changes to the Program, as necessary in the opinion of the Board of Directors, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommendations coming from the Oversight Committee will be forwarded to the Board of Directors for consideration annually. The Board of Directors is responsible for reviewing these reports and recommendations prepared by the Oversight Committee and address any recommended material changes to the Program.
    1) The Oversight Committee designated by the Board of Directors will report to the Board of Directors at least semi-annually, on compliance with the red flag requirements. The report will address material matters related to the Program and evaluate issues such as:
        a. The effectiveness of the policies and procedures of the PAMDWCA in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
        b. Service provider arrangements;
        c. Significant incidents involving identity theft and management's responses;
        d. Recommendations for material changes to the Program up for review annually.

11. Outside Service Providers.

In the event that the PAMDWCA engages a service provider to perform an activity in connection with one or more covered accounts, the Board of Directors shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft. The Board of Directors may warrant the assistance of the Oversight Committee, or the Association attorney for any questions that may arise.

12. Treatment of Address Discrepancies.

At the present time the PAMDWCA is not using consumer credit reports. If in the future the PAMDWCA begins to use consumer credit reports, the Association will comply with federal regulations regarding treatment of address discrepancies. In the event that the PAMDWCA receives a notice of address discrepancy, the PAMDWCA employee responsible for verifying Association Member addresses for the purpose of providing the municipal service or account

sought by the consumer credit agency shall perform one or more of the following activities, as determined to be appropriate by such employee:

A. Compare the information in the consumer report with:
    1) Information the PAMDWCA obtains and uses to verify a Association Member's identity in accordance with the requirements for the Association Member Information Program rules implementing 31 U.S.C. § 5318(1);
    2) Information the PAMDWCA maintains in its own records, such as applications for service, change of address notices, other Association Member account records or tax records; or
    3) Information the PAMDWCA obtains from third-party sources that are deemed reliable by the relevant PAMDWCA employee; or
B. Verify the information in the consumer report/Association Member account with the Association Member.

13. Furnishing Consumer's Address to Consumer Reporting Agency.

A. In the event that the PAMDWCA reasonably confirms that an address provided by a consumer to the PAMDWCA is accurate, the PAMDWCA is required to provide such address to the consumer reporting agency from which the PAMDWCA received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:
    1) The PAMDWCA is able to form a reasonable belief that the consumer report relates to the consumer about whom the PAMDWCA requested the report;
    2) The PAMDWCA establishes a continuing relation with the consumer; and
    3) The PAMDWCA regularly, and in the ordinary course of business, provides information to the consumer reporting agency from which it received the notice of address discrepancy.
B. Such information shall be provided to the consumer reporting agency as part of the information regularly provided by the PAMDWCA to such agency for the reporting period in which the PAMDWCA establishes a relationship with the consumer.

14. Methods of Confirming Consumer Addresses.

The PAMDWCA employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:
    1) Verifying the address with the consumer;
    2) Reviewing the PAMDWCA's records to verify the consumer's address;
    3) Verifying the address through third party sources; or
    4) Using other reasonable processes.

APPENDIX A

A. "PAMDWCA" means the Pinos Altos Mutual Domestic Water Consumers Association.
B. "Covered Account" means (1) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile, loan, margin account, cell phone account, **utility account or Municipal Court imposed fine or cost**, checking account, or savings account; (2) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to Association Members or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
C. "Credit" means the right granted by the creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.
D. "Creditor" means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and **includes utility companies** and telecommunications companies.
E. "Association Member" means a person that has a covered account with a creditor.
F. "Association Member Service Representative" (CSR) means an individual working for the PAMDWCA whose principal responsibilities include attending to Association Members and their needs.
G. "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any,
    1) Name, social security number, date of birth, official State or government issued driver's license, alien registration number, government passport number, employer or taxpayer identification number;
    2) Unique electronic identification number, address or routing code; or
    3) Telecommunication identifying information or access device.
H. "Identity theft" means a fraud committed or attempted using identifying information of another person without authority.
I. "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
J. "Oversight Committee" means the Committee appointed by the PAMDWCA to oversee operation and compliance of the PAMDWCA's ITPP in accordance with the requirements of the Fair and Accurate Credit Transaction Act.
K. "Personal Identifying Information" means a person's credit card account information, debit card account information, bank account information, and driver's license information; and for a natural person includes their social security number, mother's birth name, and date of birth.
L. "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
M. "Service provider" means a person that provides a service directly to the PAMDWCA.

APPENDIX B
(Association Member Application)

Revised Application Inserted Here

PINOS ALTOS MUTUAL DOMESTIC WATER CONSUMERS' ASSOCIATION

P.O. Box 1798
Silver City, NM 88062-1798
(575) 654-6461
bookkeeper@pamdwca.org

Application for Membership (revised 02/13/2019)

Property Owner Name _____

Contact Number: _____ Email Address _____

Mailing Address _____

Proposed Service Address _____

Does the property currently have a water meter? ____ Meter Number _____

Current Water Source _____

Number of Residences _____ Is this application for domestic use only? _____

Description of non-domestic activities _____

Description of commercial activities _____

Description of septic waste system _____

Septic system NMED inspection/approval date: _____

All new service connections or membership transfers require a shut off valve (preferred 1-2 feet from meter) to be installed and paid for by the new Association Member. The new member agrees to have one installed within 60 calendar days. Proof must be provided to the bookkeeper within 60 days or water service will be terminated. Please see the operation policy to see the current reconnect charge.

The applicant has read and understood the Association's Operations Policy, Bylaws and Articles of Incorporation, which were obtained either at http://pamdwca.org, or from the Association's business office; if granted membership in the Association, the Applicant agrees to accept and abide by these documents. All signatures necessary for the Property Owner to make this application are required below:

Applicant Signature _____ Date _____

Applicant Signature _____ Date _____

Fees required at this time include the membership fee and the security deposit.

Required Attachments:
1. Proof of ownership
2. All fees as per Operations Policy

[for office use only: _____Account number, _____Security Deposit, _____Fee]

APPENDIX C
(FORMS)

Report of Suspected Identity Theft

Reporting Party: _____ **Date/Time of Filing:** _____

Association Member Name: _____

Account Address: _____

City/State/Zip: _____

Billing Address: _____

City/State/Zip: _____

Circumstances of the Suspected Identity Theft. Please provide all relevant details.

_____

_____

_____

_____

****

Confirmation of Association Member's Identity

Presentation of approved photo identification (copy attached) _____

Completed FTC Identity Theft Affidavit (copy attached) _____

Filed police report (copy attached) _____

A written police report was not taken, but a case file number was assigned _____

Case File # _____

Officer/Agent verifying the Case File # _____

I hereby acknowledge that the information I have provided is accurate and complete to the best of my knowledge.

_____ _____

Association Member's Printed Name Signature

Date _____

Red Flag Event Log

Date _____ Time _____

Red Flag Event (describe): _____

_____

_____

Person Reporting Event: _____

Investigating Person: _____

Immediate Actions Taken in Response to Event:

1) _____

2) _____

3) _____

4) _____

Notification of Appropriate Personnel (state who and time of notification):

1) _____

2) _____

3) _____

Investigation Findings of Incident:

_____

_____

_____

Determination of Loss of Association Member Information:

_____ No Loss _____ Loss may have/did occur

Mitigating Action(s) Taken:

1) _____

2) _____

3) _____

As Required, Actions Taken to Notify Affected Association Members:

1) _____

2) _____

3) _____

Proposed Changes to Processes, Procedures, Policies to Limit Potential of Loss.

_____

_____

_____

_____ _____

Investigating Person Signature Date