# Agenda Report

October 20, 2008

**To:** City Council

**From:** City Manager

**Subject:** Water and Power Department Compliance with Fair and Accurate Credit Transactions Act

**RECOMMENDATION**:

It is recommended that the City Council approve an Identity Theft Prevention Program for the Water and Power Department (Department) to protect customer identification and credit information in compliance with the Fair and Accurate Credit Transactions (FACT) Act of 2003 and the Red Flag Identity Theft Prevention Program requirement.

**BACKGROUND**:

***FACT Act***

In 2003, Congress adopted the FACT Act and the Federal Trade Commission (FTC) developed regulations to set standards for safeguarding sensitive customer information for various entities, including utilities. On November 1, 2007, the Red Flag Identity Theft Prevention Program (Red Flag) was added to impose certain obligations on creditors for prevention, detection, and mitigation of identity theft. To create a uniform system to protect consumer credit information in compliance with the FACT Act, the FTC has issued rules for applicable financial institutions and creditors known as "Red Flag Rules." Red Flags are warning signs of patterns, practices, or specific activities associated with identity theft. The program requires creditors to positively identify each customer and to provide for the secure handling of personal customer data at all times during and after transactions with any customer. The Red Flag refers to specifically identified potential warnings of identify theft to which creditors must be aware and responsive as outlined below:

- Alerts, notifications or warnings from consumer reporting agency (Experian, Equifax, TransUnion)
- Suspicious documents
- Suspicious personal identification information
- Unusual use or suspicious activity related to a covered account
- Notice of theft from customers, victims, or law enforcement

***Role of Water and Power Department***

The FACT Act provisions regarding protection of consumer credit information apply to public utilities such as the Department and its customer accounts that are designed to permit multiple payments or transactions using a credit card, debit card or bank account information. As defined in the FACT Act, the Department is defined as a creditor because it processes requests for service and provides electric and water services in advance of receiving payment.

The Red Flag requires the Department to have a plan in place by November 1, 2008 that includes policies and procedures which meet the standards outlined by the FTC. The proposed plan is included as Attachment A to this report. The proposed plan includes identification of the potential warnings of identify theft and monitoring activities in which Department staff will participate to protect its ratepayers from identify theft. Some of these activities include the monitoring of accounts, contacting the customer to verify information and/or activities; changing procedures for passwords and security codes for both customers and employees; closing accounts in question and opening a new account once information is verified and notification of law enforcement of suspicious activity or information. The proposed plan encompasses all services provided by the Department that are included on the utility bill.

Another requirement of the Red Flag is to establish an oversight committee and administrative process to implement and report on results of the program. Staff recommends that the Municipal Services Committee be established as the oversight committee for this program and that the General Manager of the Department (or designee) serve as the administrator of the program. Staff will then be required to provide quarterly reporting of program results to the General Manager and annual reports to the Municipal Services Committee to insure compliance with the requirements of Red Flag, current privacy laws and directives for securing personal data. Any changes or updates to the policy will require City Council approval.

**FISCAL IMPACT:**

Sufficient funds are available from the Power Customer Service fund account 8114-401-833500-0910 for $25,025 and Water Customer Service fund account 8114-402-833500-0773 for $13,475 to cover costs for additional training and materials for staff and initial third party vendor Positive ID validation.

Respectfully submitted,

Michael J. Beck
City Manager

Prepared by:

for Shari Thomas

Shari M. Thomas
Business Unit Director
Water and Power Department

Approved by:

Phyllis E. Currie
General Manager
Water and Power Department

# Attachment A

FACTAct – Red Flag Identity Theft Prevention Program
Pasadena Water and Power
Policies and Procedures
Effective November 1, 2008

---

**Background:**
The Federal Trade Commission rule under the Fair and Accurate Credit Transactions Act (FACTAct) requires entities, which affect consumer credit, to evaluate and create a formal program to detect, prevent, and mitigate identity theft by November 1, 2008. The Act focuses on "RED Flags" which is defined as patterns, practices, or specific activities that indicate possible existence of identity theft on a covered account.
The program put in place by PWP must:

1.) Identify "Red Flags" for covered accounts and incorporate those "Red Flags" into the program
2.) Detect "Red Flags" that have been incorporated into the program
3.) Respond appropriately to any "Red Flags" that are detected to prevent and mitigate identity theft
4.) Ensure the program is updated periodically to reflect changes in identity theft risk to customers or the creditor
5.) Provide for administration of the program and report to Council annually

**Red Flags**:
"Red Flags" are defined as patterns, practices, or specific activities that indicate the possible existence of identity theft. The "Red Flags" that are pertinent to utilities are:

- Inclusion of a fraud or active duty alert with a consumer report
- Notification by a consumer reporting agency of a credit freeze in response to a request for a consumer report
- Documents provided for identification that appear to have been altered or forged
- Suspicious personal identification information, including failure to provide all required person identification information
- Notification of unauthorized charges in connection with a customers account
- Notification by a customer, a victim of identity theft, a law enforcement agency, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

**Red Flag Detection:**
Notices from consumer reporting agencies on customer credit freezes, unverified bank information provided for bank draft payments of utility bills, unauthorized charges to an account, and customer failure to provide either a Social Security Number, Driver's License Number, or U.S. Passport number are typical examples of "Red Flags" that will require action by PWP. This action could result in further investigation into the customer account to determine if identity theft has occurred and/or the freezing of the account.
If any of these "Red Flags" occur at the initiation of service, service will not be started until the customer supplies information that can be validated.

## I. Purpose:

The goal of this policy is to detect, prevent, and mitigate identity theft. Pasadena Water and Power (PWP) recognize the responsibility to safeguard personal customer information within the workplace. The purpose of this policy is to create an Identity Theft Prevention Program utilizing guidelines set forth in the Federal Trade Commission Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (FACTAct Red Flag Policy 2003).

## II. Scope:

This policy applies to all employees of Pasadena Water and Power, other City employees and 3rd party vendors who handle payments or have access to the billing system and personal customer data entrusted to PWP. The FACTAct Red Flag Policy supplements existing Federal and State Laws pertaining to Privacy Protection.

## III. Responsibility:

PWP must protect customer data and implement a plan including policies and procedures that meet standards established by the Federal Trade Commission, FACTAct "Red Flag" by November 1, 2008.

## IV. Definitions:

Identity Theft – Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, drivers' license, etc) with the intent of conducting transactions to commit fraud that results in substantial harm and/or inconvenience to the victim. This fraudulent activity may include opening utility accounts using fraudulent checks and/or credit cards to make payments.

Red Flag – A pattern or particular specific activity that indicates the possible risk of identity theft.

## V. FACT ACT Red Flag Procedures:

### A. Implementing the Program

1. Form an Identity Theft protection Committee

   Establish an identity theft prevention committee to create, drive and monitor the program. Select member from Senior Management, Finance, and other departments that are directly related to employee hiring and protection of customer data such as Human Resources, Customer Service, Information Technology, Law Enforcement, and City Attorney.

2. Assign Responsibilities to Committee Members

   Responsibilities should be directly related to the individual members area of expertise.

3. Appoint a Privacy Officer

The Privacy Officer functions as the head of the committee. He/she reports to a member of Senior Management (General Manager, City Manager, or City Council) regarding the outcomes and needs of the identity theft prevention program.

B. Assess Utilities Need for New/Updated Policies and Procedures

Red Flag Procedures – Steps to Detect, Prevent, Mitigate Identity Theft in New and Existing Accounts.

1. Breach of Security

To prevent identity theft by utility employees, City employees, or 3rd party vendors, limit exposure of secured information by creating a consistent, professional policy standard.

Implement a "need to know" policy with all confidential information.
Train management to recognize signs of employee theft including: sifting through waste receptacles, not following document shredding procedures, downloading excessive amounts of consumer information to a CD or mass storage device, using secured terminals without authorization, not following Personal Computer security protocol such as setting a password for screen time-out.
Train managers and supervisor the proper way to handle a Security Breach when they either discover a breech or a breech is reported to them that is consistent with the FACTAct Red Flag process, State, and Federal Law.

2. Record and Document Disposal:

Implement a record and document handling policy for all paperwork that contains customer personal data.

a.) a records retention policy for all records that must be kept for a period of time for accounting purposes.
b.) maintain a record of document destruction
c.) a destruction policy that deals with daily paperwork and/or transactions, notes, printouts, that contain personal customer information that must be destroyed on a daily basis.

3. Hiring, Screening, Training:

Run background checks on all new employees. Thoroughly screen all applicants and create specific scenario questions to ask during the interview process.

Train employees to identify Red Flags. Following the "need to know" rule, employees will receive only the information that relates to their specific job.

Supervisory training will involve additional information including identity theft prevention.

Training material includes an Identity Theft Prevention Program Manual, one for employees and one for supervisors.

4. Handling Address Discrepancies:

Occasionally, a person or agency requests a consumer report on one of PWP customers. If this report includes an address that substantially differs from the addresses in the customer's file, and a response to the request is issued, PWP should notify the person making the request of this discrepancy.

5. Handling Reports of Suspected Identity Theft:

a.) when the customer/consumer suspects Identity Theft, they must notify the Police Department and PWP in writing using the appropriate form.

b.) make a copy of customer/consumers ID and attach it to the Police Report along with the completed form and send the completed forms to the privacy officer.

c.) close or block breached account and open a new account.

d.) place an alert on the customer file and send information and to the Hold Transactions Excel Sheet to notify Customer Service of the situation.

e.) **IT IS CRITCAL THAT NO INFORMATION BE GIVEN TO THE CONSUMER UNTIL THE INVESTIGATION IS COMPLETE.** The privacy officer will determine the course of action at this point.

Victim Record Request:

Under the FACTAct, identity theft victims are entitled to a copy of the application or other business transactions records relating to their Identity theft free of charge. PWP must provide these records within 30 days or sooner of receipt of the victim's request. Businesses must also provide these records to any law enforcement agency which the victim authorizes.

If the organization does not have a high degree of confidence that it knows the victim, before providing the records, PWP must ask victims for:

a.) proof of identity, which may be a government-ID Card, the same type of information the identity thief used to open or access the account, or the type of information business is currently requesting from the applicant or customer.

b.) a police report and a completed affidavit, which ay be either the FTC Identity Theft Affidavit or the business's own affidavit.

6. IT Security:

The network administrator and IT Management will conduct audits on a quarterly basis using the Identity Theft Prevention Program Checklist for Information Technology. All Systems administrators and IT Staff shall sign agreements to not disclose private customer information.

7. Medical Confidentiality:

PWP shall not obtain or use medical information pertaining to a consumer in connection with any determination of the customer's eligibility, or continued eligibility for services. All medical information will be treated as confidential and in compliance with state and federal law.

8. Report, Reviews, Updates for Policy Enforcement:

Periodically, internal staff who report to the board, external auditors, and government regulators will review practices to ensure compliance with this policy. The reports will be used to evaluate effectiveness of and amend the Identity Theft Prevention Program. An annual report review of all incidents, program revisions, and goals will be submitted to the City Council.

## VI. Pasadena Water and Power Identity Theft Prevention Program:

Policy: PWP complies with the FACT Act by:

### A. Opening, transferring, closing a Utility Account:

Current Process:

Upon opening, transferring or closing customer accounts whether by phone or in person, current procedures require the applicant (and spouse, if the account is opened in both names) to provide either his/her/their Social Security Numbers (SSN) or Driver's License Number (DLN). For residential customers, if the SSN or DLN is not available, identification requirement defaults to the U.S. Passport Number. For commercial customers, the required identification is the Tax Identification Number (TIN). If the customer does not have or does want to give their SSN or DLN then a deposit is required to start service. Currently there is no 3rd Party Credit Checking or Positive ID Check done. DLN are checked via ultra violet light to insure they are valid.

FACTAct Red Flag Process Change:

Upon opening, transferring or closing customer accounts whether by phone or in person, FACT Act procedures will require the applicant (and spouse, if the account is opened in both names) to provide either his/her/their Social Security Numbers (SSN) or Driver's License Number

(DLN). Their social security number will be verified through a 3rd Party vendor to confirm Positive ID. For residential customers, if the SSN or DLN is not available, identification requirement defaults to a Government issued ID, such as a U.S. Passport Number. For commercial customers, the required identification is the Tax Identification Number (TIN). If the customer does not have or does want to give their SSN or DLN the customer will have to show Picture ID at the City Hall Payment Center and a deposit is required to start service. Unacceptable forms of Picture ID are Student ID or Work ID.

**B. Credit Card and Payment Processing:**

Credit Card Processing – In Person:

Credit Card Processing performed by Employees with the customer present will ask for picture identification along with the credit card to match the customer name with the name on the credit card. The credit card transaction takes place via a credit card terminal and prints a two-copy transaction receipt one for the utility's records and one for the customer. The transaction receipt displays the last 4 digits of the credit card only. The receipts are kept in a locked file for 6 months and shred. No Credit card numbers are kept in the Billing System for recurrent payments.

Credit Card Processing – By Phone:

Customers who complete their credit card transaction over the phone using the automated service receive a confirmation number from the system. No credit card information is kept in the billing system. The IVR Credit Card Report records the transaction date, customer account number, last 4 digits of the credit card number and the transaction amount. These records are part of the IVR System and are accessible to only those staff that have a need to know or work with automated payments. Customers who do not complete their credit card transaction while in the automated phone system and transfer to a representative for completion of their payment are handled through the bank credit card terminal. The Customer Service Representative (CSR) takes the customer credit card number with the security number and expiration date and payment amount enters it into the credit card terminal. The CSR either will receive an approval or denied status. If the credit card is approved the CSR will give the customer the approval number and enter the dollar amount and approval number into the customer account. Any paperwork with the full credit card number is then shred on the spot. Only paperwork with the approval number and dollar amount are kept for daily balancing. These records are in a locked file and shed in 6 months.

WEB Payments (IWR- PWPWeb.com):

Customers who use the PWPweb.com (IWR) web site to make utility payments sign-in with their account number and Personal Identification Number (PIN). Customers access their account information and enter the dollar amount that they wish to pay. The customer either will receive an approval or denied status. If the credit card is approved the customer will see the approval number and the dollar amount paid. The IWR Credit Card Report records the transaction date, customer account number, last

4 digits of the credit card number and the transaction amount. These records are part of the IVR System and are accessible to only staff that has a need to know or work with automated payments. No credit card numbers are kept in the billing system or WEB system for recurrent payments.

Direct Payment by Banks, Online Banking, Electronic Fund Transfer

Utility payments made via Banks, Online Banking, Electronic Fund Transfer are received in the Customer Service Center daily. These payments arrive from each vendor as a list of payments with account numbers, and dollar amounts. These payments are entered into the Billing System manually. If the account numbers do not match the information in the billing system the payment is sent back to the vendor to rectify with the customer.

Customers who use PWP's Direct Debit program to make utility payments complete a direct Debit application authorizing PWP to take funds from their checking account. PWP will take the utility payment from the customers checking account 10 days after the customer bill date. These records are kept in a locked cabinet and only those employees with a need to know are allowed access to process these payments. The paper records are shred after one year. Only the last four digits of the routing number are retained in the billing system to process the customers payment.

C. **Records Destruction Program:**

PWP Records Destruction Program has several levels and time frames based on the type of document and how long it needs to be retained for business purposes. Locked shred bins are in place at the Customer Service Center, Payment Center, and Meter Reading Services. Locked Shred Bins are picked up every other week by a 3rd party vendor and Shred. Shred machines are located in each department to insure immediate destruction of information that is not needed for the customer file.

First level:
Daily work that is put into designated bins at each desk. Anything that contains written notes or sensitive customer information is put into the 3rd party locked shred bin.

Second Level:
Sensitive data, that are retained for business purposes or is mandated by law to retain for any period of time is rotated out at its retention time and is put directly into the 3rd party locked Shred Bin for destruction.

D. **Customer Information System – ECIS:**

The Enterprise CIS (ECIS) is the core customer service, billing, credit/collections, software used by PWP. ECIS is used for billing utility customers for Electric, Water, Sewer, and Refuse. Additionally, there is a module for Electric and Water Meter inventory, which is used by the respective meter shops and by Refuse for trash bin inventory. The system

also generates Field Service Orders for Meter Reading, Meter Repairs, and other services.

The customer information system stores customer data for: Account Number, Name, Service Address and Mailing Address, City, State, Zip, Social Security Number, Drivers License, Phone Numbers, PIN number, last four of the check routing number, Route Number, Premise Number, Meter Reads, usage, meter numbers, billing determinants, rates, usage history, payment history, credit/collection history.
ECIS is not used to store credit card numbers or to make recurring credit card payments. The last 4 digits of Check Routing information is retained in the system for recurrent Direct Debit payments.

E. **Privacy Committee**

Privacy Committee:

| | |
|---|---|
| Privacy Officer: | PWP Finance Director |
| Privacy Team: | PWP Customer Service Manager |
| | PWP Credit Collection Supervisor |
| | PWP IT Manager/IT Security Manager |
| | Municipal Service Manager/Supervisor |
| | Public Works Refuse Manager/Supervisor |

F. **Risk Assessment:**

During our Risk Assessment the following areas were found to place PWP at Risk of Identity Theft.

1.) ECIS - No Security Masking of:
   a.) Social Security Number
   b.) Drivers License Number

2.) No Third Party tool to validate Positive ID with Social Security Number

3.) Secure work areas such as the PWP Customer Service Center, Municipal Services Payment and Cashiering area so no unauthorized employees or visitors have direct access to areas that contain customer information

4.) New Employee Confidentiality Agreement and Background Check.

G. **Needs Assessment:**

PWP has determined that the following items must be addressed to fully meet the requirements of the FACTAct Red Flag

1.) Masking of Social Security and Drivers License Number in the billing system allowing viewing of last 4 digits only

2.) Contract with a 3rd party vendor for Positive ID and Credit Check to confirm customer ID

3.) Move camera in City Hall Municipal Services room N106 so customers are completely visible through the security glass

4.) Along with a background check on all new employees, each employee must sign a confidentiality agreement that they will not disclose in any manner the personal identity of a customer to anyone at anytime.

H. **Training:**

Formal training of employees and supervisors will consist of an initial two hour training program with annual follow-up training. If laws or procedures training will be conducted as needed. Employees and supervisors will each receive a workbook that outlines the processes to be followed to detect, prevent and mitigate identity theft in compliance with the FACTAct Red Flag.

I. **Existing City of Pasadena Policy**:

In addition to the new Red Flag Rules PWP recognizes that Identity Theft could take place by an internal employee using internal systems and resources. The Electronic Media Policy as part of the Red Flag Training.

A. Manual of Personnel Rules, Practices & Procedures Section 1.00 Personal Conduct and Standards of Employment, Subject 1.40 Discipline Policy, in particular

I. Paragraph B. Causes for Disciplinary Action

25. Unauthorized release of confidential, sensitive or personal information that may be obtained by employees in the course of employment.

B. Manual of Personnel Rules, Practices & Procedures Section 1.00 Personal Conduct and Standards of Employment, Subject 1.50 Electronic Media Policy, in particular:

III. Acts which Violate the Policy

E. Malicious use.

I. Printing, downloading, saving on computer disk (whether internal or external, CD, tape, floppy disk), or otherwise duplication any communication prohibited hereunder.

J. Sending a communication that the sender knows, or reasonably should know, violates any law of the United States or the State of California, or which violates any provision of the City of Pasadena Manual of Personnel Rules, Practices & Procedures.

O. Accessing the networks, computers, electronic devices, electronic information or communications of other employees or the City of Pasadena without the express authorization from the employee who has the responsibility for maintaining said devices or information, or the Department Head of the employee seeking said information.

P. Revealing or disclosing to another, gathering, storing or disseminating in any fashion any passwords, PIN Codes credit card numbers, or other confidential information, which belongs to the City of Pasadena with the express authorization of the Department Head or his or her designee.