RESOLUTION NO._____
RESOLUTION OF THE COUNCIL OF THE CITY OF PALO ALTO
APPROVING THE CUSTOMER IDENTIFICATION AND CREDIT
INFORMATION PROTECTION PROGRAM IN COMPLIANCE
WITH THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT
OF 2003

WHEREAS, the Federal Trade Commission (FTC) rule under the Fair and Accurate Credit Transmissions Act (FACT Act) requires entities which affect consumer credit to evaluate and possibly create a formal program to detect, prevent, and mitigate identity theft before November 1, 2008; and

WHEREAS, a public utility is considered to offer or maintain accounts covered under the FACT Act; and

WHEREAS, the City of Palo Alto Utilities (CPAU) has conducted a risk assessment to determine whether the accounts it maintains are subject to a reasonably foreseeable risk of identity theft, including a review of (1) the methods used to open accounts, (2) the methods of accessing accounts, and (3) previous experiences with identity theft: and

WHEREAS, CPAU has identified relevant “red flags” defined as patterns, practices or specific activities that indicate the possible existence of identity theft; and

WHEREAS, CPAU has reviewed its processes for opening, maintaining and accessing covered accounts; and

WHEREAS, there have been no known cases of attempts at unauthorized access to customer identity and account information; and

WHEREAS, CPAU has identified new processes either for immediate implementation or for implementation in conjunction with the SAP-based customer information system scheduled to be online in 2009.

NOW, THEREFORE, the Council of the City of Palo Alto does RESOLVE as follows:

SECTION 1. The Council hereby approves the attached program “Procedures for Customer Credit Security” which is also attached to the memorandum from staff to the Utilities Advisory Commission, dated September 3, 2008.

//

//
SECTION 2. The Council finds that the adoption of this resolution does not constitute a project under Section 21065 of the California Environmental Quality Act and the CEQA Guidelines and, therefore, no environment assessment is required.

INTRODUCED AND PASSED:

AYES:

NOES:

ABSENT:

ABSTENTIONS:

ATTEST:

__________________
City Clerk

__________________
Mayor

APPROVED AS TO FORM:

__________________
Deputy City Attorney

__________________
City Manager

__________________
Director of Utilities

__________________
Director of Administrative Services
MEMORANDUM

TO: UTILITIES ADVISORY COMMISSION
FROM: UTILITIES DEPARTMENT
DATE: SEPTEMBER 3, 2008
SUBJECT: RECOMMENDATION TO APPROVE A PROGRAM TO PROTECT CUSTOMER IDENTIFICATION AND CREDIT INFORMATION IN COMPLIANCE WITH THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003

REQUEST
Staff requests that the Utilities Advisory Commission recommend that the City Council adopt changes to existing policies and procedures to comply with regulations issued by the Federal Trade Commission in the Fair and Accurate Credit Transactions (FACT) Act of 2003.

BACKGROUND
In accordance with the FACT Act, the City of Palo Alto Utilities Department (CPAU) must determine whether its covered accounts are subject to a risk of identity theft, and, if necessary, implement a consumer credit protection program designed to detect, prevent, and mitigate identity theft in customer accounts. The program should incorporate existing policies and procedures where applicable, and provide for continued administration of consumer credit protections. CPAU may tailor its program to a level commensurate with the nature and complexity of its size and activities. Such a program must be approved by November 1, 2008 by the City Council, or an appropriate subcommittee of the Council, that must be involved in the oversight, development, implementation, and administration of any program. Additionally, staff must create, at least annually, a report on its compliance with the FACT Act.

CPAU and the Administrative Services Department’s Information Technology Division have had policies and procedures in place for many years to safeguard customer identity, account information and financial transactions associated with customers' utilities accounts. In conjunction with a current effort to replace CPAU’s decade-old Customer Information System (CIS), that is no longer supported by the vendor and requires replacement, CPAU has reviewed the business practices, policies and procedures for protecting customer credit information in the areas of customer service, billing, financials, and online account management. The review identified changes, which, when implemented, will increase data security, automate manual processing, establish electronic audit trails by tracking history for all activities, and improve reporting capability, all of which serve to protect the customer credit information as required by the FACT Act.

FACT Act and the Federal Trade Commission
The Fair Credit Reporting Act (FCRA) is the primary federal law regulating consumer credit information. The FACT Act amended FCRA by allowing consumers to request one free credit
report per year, allowing consumers to monitor their credit histories, and requiring specific protections of consumer credit information. The FACT Act provisions regarding protections of consumer credit information apply to public utilities, such as CPAU, and its customer accounts that are designed to permit multiple payments or transactions.

In order to create a uniform system to protect consumer credit information in compliance with the FACT Act, the Federal Trade Commission (FTC) has issued rules and regulations for applicable financial institutions and creditors known as the “Red Flags Rules.” “Red flags” are warning signs, including patterns, practices, or specific activities, that are indicative of identity theft. The proposed program includes a description of relevant FACT Act “red flags,” “red flag” detection activities, “red flag” responses, and a section addressing program updates and administration and is attached as Attachment A. Attachment A is designed as a section to be incorporated in a Customer Service Training Manual for use in training users on the new SAP/CIS in 2009.

DISCUSSION
Red Flags:
The five categories of “red flags” are: (1) alerts, notifications, or other warnings received from consumer reporting agencies or service providers; (2) presentation of suspicious documents; (3) presentation of suspicious personal identifying information; (4) unusual use of, or other suspicious activity related to, an account; (5) notice from customers, victims of identity theft, or law enforcement activities.

Responses to Red Flags:
A wide range of policies and procedures may appropriately respond to “red flags,” and the response selected will depend on the degree of risk posed by each “red flag.” Such responses may include, but are not limited to, the following: the monitoring of accounts; contacting the customer to verify information/activities; changing protocols for passwords and security codes; closing of accounts in question and reopening accounts with verified information; refusal to open an account; refusal to collect on a suspicious account; and notification of law enforcement of any suspicious activity or information.

Risk Assessment of Utility Accounts and Procedures:
The FACT Act requires that CPAU conduct a risk assessment to determine whether the accounts it offers or maintains are subject to a reasonably foreseeable risk of identity theft, whether that risk is to the customers or to the creditor itself.

The FTC rules identify 26 “red flags.” Many of the “red flags” are more applicable for creditors that extend credit to customers for services that can be used anywhere, such as through credit cards or cell phones. Some of the “red flags” which deal with illegal use of available credit for cash advances, use of an account in a manner that is not consistent with established patterns of activity on the account, a fictitious address, or failure to meet “challenge questions” used in authenticating customer information are directly suited to other types of services such as credit card or cell phone services, but are not necessarily a major risk for utilities services. In the case of utilities accounts, service is provided to a specific address and the service itself cannot be
easily transferred (except by physical and illegal connection, constituting theft of service, but not necessarily identity theft) to another address.

Customer identifying information, however, is retained in the CIS, and this information could be subject to theft. Those "red flags" that are of relevance to the CIS maintained by the City of Palo Alto 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 identifying information including failure to provide all required personal identifying information;
- Notification of unauthorized charges in connection with a customer's account;
- Notification by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft;

Current CPAU Customer Billing Procedures:
Current billing procedures require the applicant (and spouse, if the account will be opened in both names) to provide either his/her/their Social Security Numbers (SSN) or Driver's License Numbers (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). All SSN and TIN are masked except for the last four digits. Customers can currently access some of their account information, including the name on the account, address, consumption data, meter reads, dates of service, charges, billing adjustments and payments via customer-specific and customer-identified login ID, customer created password, CPAU account number, and customer name. Currently, customers' on-line transactions are limited to establishing or modifying an e-mail address, establishing or updating a phone number, and sending a customer note regarding account information to CPAU. CPAU's staff access to the CIS is role-specific, and depending on the role, only certain functions within CIS can be accessed following review and approval by CPAU's Customer Service Manager.

Other existing account protections are already in place. For customers paying by bank draft, the voided checks are kept in a locked cabinet and maintained per the City's Records Retention Policy. For customers paying by credit card, receipts only contain the last four digits of the credit card number and no expiration date is included in the printout of the receipt. It is proposed that the existing protections be continued as part of the City's FACT Act response, and an improvement will be promptly recommended for immediate implementation. Such an improvement could consist of the requirement that shredding of all customer account documents shall occur once they are no longer needed.

Creditworthiness Review Improvements:
The current policy and procedure to establish and maintain creditworthiness will also be evaluated. This evaluation will determine if the widely-used FICO scoring systems established
and maintained by the three major credit rating agencies (Experian, TransUnion and Equifax) in the country can improve the ability of CPAU to detect and mitigate customer credit security “red flags” and reduce future financial risk. Implementation of the new creditworthiness procedures is scheduled to coincide with the implementation of the SAP-based CIS replacement project in 2009.

**New Procedures:**
The FACT Act also requires that if CPAU determines that its accounts may be subject to a risk of identity theft, it must design a program to detect, prevent, and mitigate that risk. As stated above, modifications or additions to an existing program are permissible, and CPAU may tailor its program to reflect the size and complexity of its business.

Many of the changes identified for implementation in the new SAP/CIS system, scheduled for Spring 2009, will improve consumer identity and credit information protections. To improve CPAU staff’s ability to monitor customer accounts, the new CIS system will: establish the City’s on-line geographic information system (GIS) as the quality controller on address accuracy for customer correspondence; limit credit card payments to single transactions, eliminating the need to store customer credit card information in CPAU’s database; protect customer bank account information through the listing of accounts by the last four digits only; create an enhanced audit trail and record of customer refunds and refund checks; and maintain records and an audit trail for reversing transactions.

**Response to Electronic or Physical Security Threats:**
To date, there have been no known attempts to compromise the existing CIS or unauthorized incidents of accessing customer information. In the event there is any indication of physical or electronic threat to customer credit or identity security, CPAU will work with the Information Technology Division, the City Attorney’s Office, and the Palo Alto Police Department as appropriate to eliminate the threat.

**Program Administration, Updates and Reporting:**
Periodic reviews, conducted at least annually, will assess the effectiveness of the policies and procedures in light of any changes in identity risks to customers or to CPAU or the City. Any program changes will be submitted to the Council for review and approval. The Director of Utilities will provide day-to-day oversight over the policies and procedures, and CPAU will report annually to the Council on the program effectiveness.

**RESOURCE IMPACT**
Any operating costs associated with the proposed program will be included in CPAU’s operating budget. Any capital costs associated with implementing changes to the program in the SAP-based CIS will be included in the appropriate CIP budget.

**ENVIRONMENTAL REVIEW**
Approval of the program does not constitute a project under the California Environmental Quality Act pursuant to California Public Resources Code Section 21065; therefore no environmental assessment is required.
ATTACHMENTS
A: DRAFT Utilities Procedures for Customer Credit Security Program
B: Federal Register/Vol. 72, No. 217/Friday, November 9, 2007/Rules and Regulations: Alerts, Notifications or Warnings from a Consumer Reporting Agency; Suspicious Documents; Suspicious Personal Identifying Information

PREPARED BY: TOM AUZENNE
Assistant Director, Customer Support Services

DEPARTMENT HEAD: VALERIE O/FONG
Director of Utilities
DRAFT

City of Palo Alto Utilities

Procedures for Customer Credit Security

In Accordance with the
Fair and Accurate Credit Transactions Act of 2003

Approved by the City Council October XX, 2008

Updated: October YY, 2008

CPAU Logo

City of Palo Alto Logo
Background

The Federal Trade Commission rule under the Fair and Accurate Credit Transactions Act requires entities, which affect consumer credit, to evaluate and possibly create a formal program to detect, prevent and mitigate identity theft before November 1, 2008. The Act focuses on “red flags” - defined as patterns, practices, or specific activities that indicate possible existence of identity theft on a covered account.

The program 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.

This section describes what “red flags” are, our “red flag” detection program, how best to respond to any identified “red flags,” and on-going administration of the program.
What are “Red Flags?”

“Red flags” are defined as patterns, practices or specific activities that indicate the possible existence of identity theft. Some of the identified red flags that are particularly pertinent in the Utilities lines of business 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 identifying information, including failure to provide all required personal identifying information;
- Notification of unauthorized charges in connection with a customer’s account;
- Notification by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft;

Customer identifying information is retained in the customer information system, and this information could be subject to theft. Those “red flags” that deal with theft of such customer information are of greater relevance to the customer information system maintained by the City of Palo Alto and are listed above.
“Red Flag” Detection

Notices from banking institutions of unauthorized charges to an account, notices from consumer reporting agencies on customer credit freezes, unverified bank information provided for bank draft payments of utilities bills, 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 either freezing of an account or further research into the customer account to determine if identity theft has occurred. If any of these “red flags” occur at customer initiation of service, service will not be established.
Response to “Red Flags”

Current Procedures
Currently, procedures are in place to protect customers’ identities from theft. Procedures will apply during the opening, transferring or closing of customer accounts. They also will apply as customer accounts and associated records are accessed. Still others apply during the billing of accounts and collection of payments. Additionally, some of the procedures that apply are initiated by Utilities staff, while others apply when customers access their own account information.

- **Masking of Customer Identity**
  Upon opening, transferring or closing customer accounts, current customer billing 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 Numbers (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 Numbers (TIN). All SSN and TIN are masked except for the last four digits.

- **Security Access to Customer Accounts and Records**
  **Customer Access:**
  Currently, in order to access account information online, customers must create a user name and password. These are controlled by the customer and account information is accessed via the “My Utilities Account” web portal. Information to which customers have access includes: the name on the account, address associated with the account; consumption data; meter reads; dates of service; charges; billing adjustments; and payments. Customers can also conduct a limited number of on-line transactions, including modifying their e-mail addresses, establishing or updating a phone number, and sending a customer note to CPAU staff regarding account information.

  **City Staff Access:**
  Currently, City staff access is role-specific, and depending on the role, only certain functions within the customer information system can be accessed following access review and approval by the Utilities Customer Service Manager.

- **Billing and Collection**
  Currently, customers choosing to pay by bank draft submit voided checks which are kept in a locked cabinet and maintained in accordance with the City’s Records Retention Policy. Customer security deposits are manually established and tracked. Receipts produced for credit card payments only contain the last four digits of the credit card, and as an added precaution, expiration date information is not included on the receipt. While it is not a
requirement, as a precautionary measure, customer information is typically shredded before being discarded.

**FACT Act Procedure Changes**
Changes or enhancements to current customer identity security procedures will either be implemented immediately, or will be enabled in the new SAP-based customer information system (SAP-CIS) scheduled to go online in 2009.

- **Enhanced Masking or Security of Customer Identity**
  Customer identity will continue to be masked except for the last four digits. SAP-CIS will contain greater flexibility in developing user roles, which will allow tighter restrictions on which users will have access to information such as "business partner" (including spouse) information.

- **Enhanced Security Access to Customer Accounts and Records**
  **Customer Access:**
  Enhanced online services under the SAP-CIS will allow customers to better manage their own accounts as a secondary flagging system for anything that might be amiss. The SAP-CIS will: permit the linking of all accounts for the same customer to a single customer-created user name and password; permit viewing and payment of bills online; permit printing of monthly bills via an online download; permit self-service move-out requests and online self-enrollment in bank drafting; and permit monthly audits of bank drafting activities.

  **City Staff Access:**
  Stricter role definitions, limiting the potential of wholesale theft of information via stolen password or City staff ID, will be allowed under the SAP-CIS. Access to changes to customer accounts will be limited to the customer service role. Other areas (Accounting) will only have the ability to view customer accounts, but will not be able to make changes, an additional security in the system. Additionally, the SAP-CIS will enable the creation of records and audit trails of reversed transactions, and will create an enhanced audit trail and record of customer refund and refund checks as a more refined tool for monitoring account activity.

- **Enhanced Billing and Collection Security Procedures**
  Enhancement for immediate implementation: The required shredding of all customer account documents prior to disposal.

In parallel with the development of the SAP-based CIS system, the Customer Services Manager is directing a review of the creditworthiness policies and is evaluating FICO scoring systems to determine their applicability to CPAU's customer creditworthiness assessments. Implementation of the new creditworthiness procedures is scheduled to coincide with the implementation of the SAP-based CIS replacement project in 2009.
Additionally, when the SAP-CIS is implemented in 2009, customer bank account information will be masked in the system, and access to unmasked information will be restricted to one or two users through “Role Definition” and authorization.

The SAP-CIS will automatically create a trail of every customer account and financial transaction to permit better identification of any red flags. The SAP-CIS will not store credit card information, reducing one of the theft targets.
Program Updates and Administration

A. General

Oversight of the program involves assigning specific responsibility for oversight, reviewing reports, and approving material changes in the program.

Material changes in the program shall be based on experience with identity theft; changes in methods of identity theft, changes in methods to detect, prevent, and mitigate identity theft, changes in types of accounts offered, and changes in business arrangements.

The Customer Services Manager shall ensure updated versions of the program are included in the Customer Service Representatives Training Manual.

B. Role of Director of Utilities

The Director of Utilities shall be responsible for oversight over program implementation. The Director of Utilities shall work with the Assistant Director of Customer Support Services and the Customer Services Manager to ensure day-to-day oversight over security of customer credit information in conformance with the FACT Act.

In the event there is any indication of physical or electronic threat to customer credit information or identity security, the Director of Utilities shall work with the Information Technology Division, the City Attorney’s Office, and the Palo Alto Police Department as appropriate to eliminate the threat.

The Director of Utilities shall submit a report at least annually to the Council, updating the Council on any material changes in the program, any customer credit security threats or actual theft of customer credit information.

C. Role of Council

The Council shall review reports submitted and consider and approve appropriate material changes to the program.
Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 41.82(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   a. A recent and significant increase in the volume of inquiries;
   b. An unusually large 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.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with the identification provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
   a. The address does not match any address in the consumer report; or
   b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
   a. The address on an application is the same as the address provided on a fraudulent application; or
   b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with a fraudulent application.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. 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 other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Suspicious Activity Related to the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
   a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
   b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered 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 increase in the use of available credit;
   c. A material change in purchasing or spending patterns;
   d. A material change in electronic fund transfer patterns in connection with a deposit account; or
   e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer’s covered account.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Board of Governors of the Federal Reserve System

12 CFR Chapter II.

Authority and Issuance

For the reasons set forth in the joint preamble, part 222 of title 12, chapter II, of the Code of Federal Regulations is amended as follows:

PART 222—FAIR CREDIT REPORTING (REGULATION V)

1. The authority citation for part 222 continues to read as follows:


Subpart A—General Provisions

2. Section 222.3 is amended by revising the introductory text to read as follows:

§ 222.3 Definitions.

For purposes of this part, unless explicitly stated otherwise:

* * * * *

3. The heading for Subpart I is revised to read as follows:

Subpart I—Duties of Users of Consumer Reports Regarding Address Discrepancies and Records Disposal

4. A new § 222.82 is added to read as follows:

§ 222.82 Duties of users regarding address discrepancies.

(a) Scope. This section applies to a user of consumer reports (user) that receives a notice of address discrepancy from a consumer reporting agency, and that is a member bank of the Federal Reserve System (other than a national bank) and its respective operating subsidiaries, a branch or agency of a foreign bank (other than a Federal branch, Federal agency, or insured State branch of a foreign bank), commercial bank or thrift association.
DRAFT

UTILITIES ADVISORY COMMISSION
MINUTES OF SEPTEMBER 3, 2008

CALL TO ORDER
Chair Dawes called to order at 7:00 P.M. the scheduled meeting of the Utilities Advisory Commission (UAC).

Present: Commissioners Dexter Dawes, John Melton, Asher Waldfogel and Council Member Yiaway Yeh
Absent: Commissioners Marilyn Keller and Dick Rosenbaum

ORAL COMMUNICATIONS
NONE

APPROVAL OF THE MINUTES
The minutes from the August 6, 2008, were unanimously approved.

AGENDA REVIEW
No changes to the agenda were requested.

REPORT FROM COMMISSION MEETINGS/EVENTS
NONE

UTILITIES DIRECTOR REPORT
Utilities Director Valerie Fong provided the following updates:

1. **FY 2008-09 and 2009-10 Budget**: Based on the latest updates of expected supply costs for the next two years, a mid-year rate increase is not being considered at this time. A presentation updating the Commission on supply costs is scheduled for the October meeting.

2. **Gas Prepay Project**: McDonald Partners has been selected to be the City’s consultant. The consultant will assist the City in evaluating the risks and rewards of various prepay structures and will assist in identifying any internal policy changes or operating requirements. One key component of the scope of work is to educate staff, the UAC and Council. Work is expected to begin in September.

3. **Marketing**: New email newsletters on energy efficiency and sustainability (developed by a third party contractor) have been implemented to inform our customers about programs and projects they can do to enhance their bottom line, reduce energy bills, and reduce GHG emissions.

4. **Drought Concerns**: Staff is working with BAWSCA to review and firm up regional mandatory drought plans, should they be required.

5. **Water Service Contract Negotiations**: Negotiations continue on a new water service contract between San Francisco and BAWSCA on behalf of the BAWSCA agencies. The latest report indicates that there are several serious challenges to having a completed contract before the current contract expires on June 30, 2009.
6. **Solar Water Heating Program:** Training for building inspectors, contractors and residents continues. The first two rebates applications under the program have been received.

7. **Energy Efficiency Rebates:** Updates to the SMART Energy (residential) and CAP (commercial) rebates have been completed to make the programs easier to understand and more similar to those offered in surrounding utilities.

8. **GHG Reduction Initiatives:** Staff has worked with the Sustainability Team extensively over the summer to provide six years of electric and natural gas history for each City utility account. The Sustainability Team will look at this information to find the best places to focus resources in the reduction of GHG. Staff has also been working with Public Works and the Sustainability Team on developing an LED Streetlight Pilot Project. Staff is coordinating with Jim Baer on his “First Wave” initiative to “green” 100 buildings in Palo Alto. A simplified “walk through” audit is being developed to enable these building managers to conduct preliminary reviews of their buildings and find the lowest hanging fruit for efficiency upgrades. Staff is also looking at potential options to integrate the PAG program with the overall efforts to reduce GHGs.

9. **Update on Solar PV Questions from Last Month’s Meeting:** Assistant Director Tom Auzenne provided the following updates:
   - Federal Investment Tax Credit (renewable tax credits) is still stalled in Congress. Will expire at the end of this year;
   - PV Program budget is $13M for 10 years, or 10 program “steps”. The rebate level of each step is at least 7% lower than prior step (per SB1 mandate);
   - There has not been a California state tax credit for photovoltaic systems since 2005;
   - (DC to AC conversion) … on average the AC rating is 75% to 80% of the DC rating.

10. **NCPA Finance Committee:** Council Member Yeh has been appointed to the Northern California Power Agency’s Finance Committee.

11. **UAC Calendar:** Fong provided a rolling calendar of upcoming items for UAC meetings. Council Member Yeh asked whether the UAC should have an expanded role in reviewing the SAP system and the IT website as a vehicle for additional on-line payment options. Staff did not render an opinion on the matter.

**UNFINISHED BUSINESS**

NONE

**NEW BUSINESS**

**ITEM 1: DISCUSSION ITEM: Frequency of Updates**

Director Fong announced that Utilities would return to its prior practice of providing quarterly updates.

Commissioner Melton advised that the content in the quarterly reports should focus on policy matters and not as much on operational aspects such as reliability impact measures. Fong noted that these impact measures would be provided annually, not quarterly.

Commissioner Dawes stated that once a system is created to produce a certain report, that the ongoing administrative burden should be small.

Commissioner Waldfogel asked that the reports should contain information and drivers that will drive quarterly decisions.
ITEM 2: ACTION ITEM: Recommendation to Approve a Program to Protect Customer Identification and Credit Information in Compliance with the Fair and Accurate Credit Transactions Act of 2003

Assistant Director Tom Auzenne explained that the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) requires that the City Council must approve a consumer credit protection program by November 1, 2008.

Commissioner Waldfogel asked about storing credit card information. Since the City only accepts one-time payments using credit cards and not recurring payments, it doesn’t need to store credit card information. The new billing system will continue this one-time, non recurring credit card payment policy. Commissioner Waldfogel said that he supports the proposed program as long as it doesn’t preclude recurring credit card payments in the future.

Commissioner Melton noted that this program is aimed at identity theft, but that on-line theft is much less common than physical theft, including laptops or media storage devices (e.g. CDs or flash drives). He asked about the current policies on access to information within the building or on carrying the information outside of the building. Auzenne noted that the current system has had no identity theft occurrences and that the new system will be an improvement due to its auditing feature that shows which Customer Service Rep has touched each customer account.

Commissioner Melton asked why the Utility needs social security numbers, driver’s license numbers or passport numbers. Auzenne replied that these numbers are used to ensure that a caller asking for information on an account is the person responsible for the account and to help find customers who have not paid.

Commissioner Dawes asked what needs to be done to implement the proposed policies. Fong responded that we will be in compliance with the new policies even if the new billing system is not on line until 2009. Auzenne added that there are no known processes or procedures in the current system that would need to be changed.

Melton moved and Waldfogel seconded the motion to “Recommend to Council approve a program to protect customer identification and credit information in compliance with the Fair and Accurate Credit Transactions Act of 2003”

ACTION: The Commission voted unanimously (3-0) to approve the motion.

The next scheduled meeting is set for October 1. Chair Dawes announced that he will not be able to attend this meeting and that he believes that Commissioner Keller will not be able to attend this meeting.

Meeting adjourned at 8:05 P.M.

Respectfully submitted,
Marites Ward
City of Palo Alto Utilities