

**COUNCIL POLICY  
TOWN OF LOS GATOS**

---

Subject: Identity Theft Prevention

Pages 1-3

---

Approved:

*Diane McNatt*

Effective Date: 12/21/2009

Revised Date:

---

**PURPOSE**

The purpose of this policy is to establish an identity theft prevention program to protect the personal and financial information of residents and businesses which have new or existing accounts with the Town as required by the federal Fair and Accurate Credit Transactions (FACT) Act. The Federal Trade Commission (FTC) and other federal regulatory agencies have recently published rules and guidelines for regulating identity theft. The new regulations implement Sections 114 and 315 of the Fair and Accurate Credit Transaction Act of 2003 (FACTA), 15 U.S.C. sections 1681a *et seq.* The FTC's rules are known as the "Red Flag Rules" (Rules), 16 C.F.R. Part 681. The Rules apply to local governmental entities that are considered to be "creditors" that maintain "covered accounts."

The FACT Act specifically applies to only "covered accounts" that involve multiple payments or transactions involving deferred payment – such as utility accounts (which the Town of Los Gatos does not have). In applying the Rules to local governmental entities, the FTC has indicated that:

- A local governmental entity providing a one-time or limited-time service for a one-time payment or a set amount of payments is not subject to the Rules.
- A local governmental entity in which a franchisee provides the utility services and the local governmental entity does not maintain the customer accounts is not subject to the Rules.
- A local governmental entity that continually collects taxes is not subject to the Rules.

This program will nevertheless be applied to other transactions (e.g. paying for one-time recreation programs, business licenses, building permits, etc.) in order to provide the broadest possible protection against identity theft.

**POLICY**

Identity theft, as defined by the FACT Act, means "a fraud committed or attempted using the identifying information of another person without authority"; with identifying information encompassing: name; social security number; date of birth; government-issued drivers license or identification card; alien registration number; passport number; employer or taxpayer

identification number; fingerprint; unique electronic identification number, address or routing code; and a telecommunication identifying access device.

A. Identification of Patterns, Practices or Specific Activities – Red Flags. The following events are considered “red flags” which suggest that identity theft may be present:

- (1) Person offers suspicious documents that appear to be altered, non-official, copied from an original, information purposely obscured, physical description does not match photo;
- (2) Suspicious personally identifying information used to open an account, such as not knowing their address for the new account, asking for basic information that should be known by the resident or business; address on application same address from previously known fraudulent account; or fails to provide all required information.
- (3) Mail sent to address is returned as undeliverable although transactions continue to be conducted in connection with the customer’s account.
- (4) Customer makes first payment and makes an initial payment, but no subsequent payments.
- (5) Town is notified that the customer is not receiving account statements.

B. Detection of Red Flags. Some of the red flags listed above will generally be detected when a person comes to the service counter to open an account, pay for a service, or undertake another type of transaction.

Town staff should review on a monthly basis, lists of accounts where payments have not been made, and should cross-check payment history to determine if one of the red flags is present.

Town staff will be contacted if a customer claims that s/he is not receiving account statements, and staff should verify payment history, when account was opened, and when last account statement was sent.

C. Response if Red Flag Triggered. If any red flags are detected, the Finance and Administrative Services Director and the Police Chief shall be notified. These staff, or their designees, shall evaluate the situation to determine if illegal activity has occurred, and take appropriate action to stop any further illegal transactions regarding the resident or business account, notify credit reporting agencies, contact person whose identity has been compromised, and take other reasonable measures, including, but not limited to: changing security codes (if

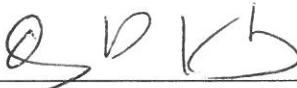
applicable), reopening the account with a new account number; not opening a new account; closing an existing account; and/or commence a criminal fraud investigation.

- D. Training of Staff and Consultants regarding Program. Town Departments which are involved in financial transactions with residents or businesses shall be provided a copy of this policy and trained regarding the identification, detection and response to red flags.

In addition, all consultants and companies which provide credit card or other financial transaction processing services for the Town shall also be provided a copy of this policy and be required to comply with these provisions, as applicable. Town staff shall collaborate with such consultants and companies to implement programs which integrate red flag detection into such services.

- E. Review of Program Annually. Every twelve months, the Finance and Administrative Services Director and other staff shall review this policy to determine if modifications are needed to address operational changes, amendment to governing law, actual experiences encountered during the prior twenty-four months, increase or decrease in covered accounts, and changes in risks from identity theft.

APPROVED AS TO FORM:

  
\_\_\_\_\_  
Town Attorney