



City of Aliso Viejo

COUNCIL POLICY

SUBJECT	RES. NO.	POLICY NO.	EFF. DATE	PAGE
IDENTITY THEFT PREVENTION AND PAYMENT CARD INDUSTRY DATA SECURITY STANDARD POLICY	2005-056	300-6	10/7/2009	1 of 5

PURPOSE

The purpose of this policy is to establish standards for the acceptance and processing of credit card payments at City facilities and maintaining the security of confidential data. This policy ensures compliance with regulations issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").

The FACTA sets forth guidelines regarding the implementation of programs to detect, prevent, and mitigate identity theft. The policy should provide for the detection of and response to specific activities ("red flags") that could be related to identity theft.

This policy is further intended to ensure compliance with Payment Card Industry (PCI) Data Security Standards, as required by the credit card companies. The standard was developed to minimize the risk of loss due to security breaches in processing credit card transactions. Non-compliance can result in fines, and/or revocation of credit card acceptances.

POLICY

Definitions

For purposes of this Policy, the following definitions shall apply:

Identity theft is defined as a fraud committed or attempted using the identifying information of another person without authority.

Confidential data shall mean information that may be used to identify a specific person, including, but not limited to, a social security number, date of birth, government issued driver's license number or identification, a government issued passport and/or unique electronic identification number.

Red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Credit is defined as the right granted by a 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 therefor.

City Staff is defined as an employee of the City or an employee at a city facility outsourced through contract services.



City of Aliso Viejo

COUNCIL POLICY

SUBJECT	RES. NO.	POLICY NO.	EFF. DATE	PAGE
IDENTITY THEFT PREVENTION AND PAYMENT CARD INDUSTRY DATA SECURITY STANDARD POLICY	2005-056	300-6	10/7/2009	2 of 5

Payment Card Industry (PCI) Data Security Standard

The payment card industry requires merchants that store, process or transmit cardholder data to comply with its *Cardholder Information Security Program (CISP)* and the *Payment Card Industry Data Security Standard*. The data security standard includes a comprehensive checklist (*Payment Card Industry Self-Assessment Questionnaire*), which can be used by merchants to evaluate controls over the protection of confidential data and personal payment card information. This self-certification is a rigorous set of best practices designed to safeguard cardholder information.

The City of Aliso Viejo will annually review and update the *Payment Card Industry Self-Assessment Questionnaire and Attestation of Compliance* as required by PCI.

Transaction Control Requirements

City staff who is responsible for completing financial transactions or is authorized to access confidential data shall comply with the following:

- 1) Prior to swiping a credit card:
 - a. Ensure the credit card has a valid expiration date. Expired credit cards must not be accepted for payment.
 - b. Compare the name on the credit card to the cardholder's photo identification. If the names do not match, the credit card must not be accepted for payment.
- 2) Ensure that the amount charged to the card matches the transaction. No refunds or credits may be issued in conjunction with the payment.
- 3) A signature must be obtained on the credit card payment slip and compared to the signed credit card or the credit card owner's photo identification. In the event of unmatched signatures, the credit card transaction must be voided and the credit card returned to the customer.
- 4) If the credit card's magnetic strip cannot be read, the card number should be keyed into the credit card terminal. To reduce the risk of access to confidential credit card data, manual imprints of the card should not be made.
- 5) If the credit card machine sends a "decline" or "no match" response, the credit card must not be accepted.



City of Aliso Viejo

COUNCIL POLICY

SUBJECT	RES. NO.	POLICY NO.	EFF. DATE	PAGE
IDENTITY THEFT PREVENTION AND PAYMENT CARD INDUSTRY DATA SECURITY STANDARD POLICY	2005-056	300-6	10/7/2009	3 of 5

- 6) In all circumstances of declined or unaccepted transactions, return the credit card to the customer and offer to accept another method of payment. Customers disputing the decline or non-acceptance of the credit card should be referred to the issuer of the card.
- 7) If you are taking a payment through the mail, make sure to obtain proper authorization. The following details should be collected from the customer on a designated authorization form:
 - a. Credit card account number
 - b. Cardholder's name as it appears on the card
 - c. Credit card expiration date as it appears on the card
 - d. Cardholder's statement address
 - e. Signature

Preventing and Mitigating Identity Theft

- 1) Credit cards should always be in your possession during transaction processing. This step provides the time needed to check the authenticity of the credit card and to compare the cardholder's signature on the credit card with the signature on the transaction receipt.
- 2) Secure all confidential data at all times.
 - a. All File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with confidential data will be locked when not in use or under supervision.
 - b. Storage rooms containing documents with confidential data and record retention areas should be locked at all times.
 - c. Desks, workstations, work areas, printers and fax machines, and common shared work areas should be cleared of all documents containing confidential data when not in use.
 - d. When documents containing confidential data are ready to be discarded they should be shredded using a mechanical shredding device. City records, however, may only be destroyed in accordance with the **City's Records Retention Policy**. Please consult with the City Clerk's office for information on the records retention schedule.
- 3) Restrict access to credit card machines, cardholder data and confidential data to authorized personnel only and in accordance with established access levels.



City of Aliso Viejo

COUNCIL POLICY

SUBJECT	RES. NO.	POLICY NO.	EFF. DATE	PAGE
IDENTITY THEFT PREVENTION AND PAYMENT CARD INDUSTRY DATA SECURITY STANDARD POLICY	2005-056	300-6	10/7/2009	4 of 5

- 4) Submission of credit card numbers (full or partial) or any related cardholder information or confidential data via e-mail is unsecure and prohibited.
- 5) For credit card transactions, paper receipts should only contain the last four (4) digits of the credit card number.

Identification of Relevant “Red Flags”

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

- Credit card and/or identification card appear to be forged or altered;
- Photograph on the credit card or identification card is not consistent with the appearance of the person presenting the identification;
- Information presented as verification is not consistent with the information on the credit card (i.e. signature appears forged);
- A customer refuses to provide a secondary identification;
- A customer notifies the City of fraudulent activity on their credit card
- An unauthorized employee requests access to cardholder information or records;
- Identifying information is presented that is inconsistent with other information provided (i.e., inconsistent birth dates);
- Identifying information is the same as submitted by someone else.

Responding to Red Flags

- 1) If one or more red flags are detected or identified, employees should gather all related documentation, write a description of the situation and provide this information to the employee’s supervisor.
- 2) The supervisor should review the documentation for fraudulent activity.
- 3) If a transaction is determined to be fraudulent, the supervisor must take appropriate action, which may include:
 - a. Canceling the transaction;
 - b. Notifying and cooperating with appropriate external agency or law enforcement; and
 - c. Determining the extent of liability to the City.



City of Aliso Viejo
COUNCIL POLICY

SUBJECT	RES. NO.	POLICY NO.	EFF. DATE	PAGE
IDENTITY THEFT PREVENTION AND PAYMENT CARD INDUSTRY DATA SECURITY STANDARD POLICY	2005-056	300-6	10/7/2009	5 of 5

- 4) If an employee discovers or reasonably suspects that credit card information has been lost, stolen or accessed without authorization, this must be reported to their supervisor immediately.
- 5) The supervisor must immediately inform the manager of the facility where the fraudulent activity occurs and the Director of Financial Services.

Administration and Oversight of the Policy

The Director of Financial Services will review and update this policy as required to address changing identity theft risks. As part of the review, red flags may be added, revised, replaced or eliminated. Updates to this Policy will require City Council action.