

# CITY OF WILLOW PARK

## ORDINANCE NO. 617-10

AN ORDINANCE AMENDING THE MUNICIPAL CODE OF ORDINANCES OF THE CITY OF WILLOW PARK, TEXAS BY PROVIDING A NEW ARTICLE 1.1900 "IDENTITY THEFT PREVENTION PROGRAM" TO COMPLY WITH CERTAIN FEDERAL REGULATIONS CONTAINED IN THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003 (PUB. L. 108-159); AND, PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, the City of Willow Park, TX ("City") is a municipal corporation organized under the laws of the State of Texas; and

WHEREAS, it is the intent of the City of Willow Park to protect the health, safety, welfare and well being of its citizens; and

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, (Pub. L. 108-159), and its implementing regulations, known as the Red Flags Rule, require certain creditors, with "covered accounts" to prepare, adopt, and implement an identity theft prevention program to identify, detect, respond to and mitigate patterns, practices or specific activities which could indicate identity theft, which are known as Red Flags; and

WHEREAS, the City maintains certain continuing accounts with customers, and for other purposes, which involve payments or transactions, and such accounts are "covered accounts" within the meaning of the Red Flags Rule; and,

WHEREAS, In order to comply with the Red Flags Rule, the City has prepared an Identity Theft Prevention Program.

NOW THEREFORE: BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF WILLOW PARK, TEXAS:

### SECTION 1. AUTHORIZATION

The Mayor, or his designee, is hereby authorized and directed to implement the applicable provisions of this ordinance.

### SECTION 2. AMENDMENT

The Municipal Code of Ordinances of the City of Willow Park, Texas, Chapter 1, "GENERAL PROVISIONS" is amended by adding a new Article

1.1900. "Identity Theft Prevention Program", as follows:

### ARTICLE 1.1900. IDENTITY THEFT PREVENTION PROGRAM

#### Section 1.1901. Purpose

The purpose of this Ordinance is to implement an Identity Theft Prevention Program as required by the Fair and Accurate Credit Transactions Act of 2003, (Pub. L. 108-159), and its implementing regulations, known as the Red Flags Rule.

#### Section 1.1902. Findings

The Federal Trade Commission ("FTC") requires every creditor to implement an Identify Theft Prevention Program ("Program") under Section 114 of the Fair and Accurate Credit Transactions Act. The Program requirements are published in 16 CODE FEDERAL REGULATIONS § 681.2.

Identity theft is defined as a fraud committed or attempted using identifying information of another person without authority. The City adopts this Program to comply with FTC rules and regulations.

In drafting this Program, the City considered: (1) the methods it provides to open its accounts; (2) the methods it provides to access its accounts; and (3) its previous experiences with identity theft. Based on these considerations, the City hereby determines that the City is a low to moderate risk entity and, as a result, develops, and implements the streamlined Identity Theft Prevention Program set forth in this ordinance.

#### Section 1.1903. Red Flags

The FTC regulations identify numerous Red Flags that must be considered in adopting an Identity

Theft Prevention Program. A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. The City identifies the following Red Flags:

a. Notifications from Consumer Reporting Agencies. The City does not request, receive, obtain or maintain information about its customers from any Consumer Reporting Agency.

b. Suspicious documents. Possible Red Flags include:

- 1) Presentation of documents appearing to be altered or forged;
- 2) Presentation of photographs or physical descriptions that are not consistent with the appearance of the applicant or customer;
- 3) Presentation of other documentation that is not consistent with the information provided when the account was opened or existing customer information;
- 4) Presentation of information that is not consistent with the account application; or
- 5) Presentation of an application that appears to have been altered, forged, destroyed, or reassembled.

c. Suspicious personal identifying information. Possible Red Flags include:

- 1) Personal identifying information is being provided by the customer that is not consistent with other personal identifying information provided by the customer or is not consistent with the personal identifying information provided by the customer or is not consistent with the customer's account application;
- 2) Personal identifying information is associated with known fraudulent activity;
- 3) The social security number (if required or obtained) is the same as that submitted by another customer;
- 4) The telephone number or address is the same as that submitted by another customer;
- 5) The applicant failed to provide all personal identifying

information requested on the application; or

6) The applicant or customer cannot provide authenticating information beyond that which generally would be available.

d. Unusual use of or suspicious activity related to an account. Possible Red Flags include:

- 1) A change of address for an account followed by a request to change the account holder's name;
- 2) A change of address for an account followed by a request to add new or additional authorized users or representatives;
- 3) An account is not being used in a way that is consistent with prior use (such as late or no payments when the account has been timely in the past);
- 4) A new account is used in a manner commonly associated with known patterns of fraudulent activity (such as customer fails to make the first payment or makes the first payment but no subsequent payments);
- 5) Mail sent to the account holder is repeatedly returned as undeliverable;
- 6) The City receives notice that a customer is not receiving his paper statements; or
- 7) The City receives notice of unauthorized activity on the account

e. Notice regarding possible identity theft. Possible Red Flags include:

- 1) Notice from a customer, an identity theft victim, law enforcement personnel or other reliable sources regarding possible identity theft or phishing related to covered accounts.

#### **Section 1.1904. Proof of Ownership**

Before changing a name and address of an existing covered account, the City requires proof of property ownership or rental such as documentation from escrow, copy of a real estate contract or deed of trust.

**Section 1.1905. Confidentiality of Applications and Account Information**

All personal information, personal identifying information, account applications and account information collected and maintained by the City shall be a confidential record of the City and shall not be subject to disclosure unless otherwise required by State or Federal Law.

**Section 1.1906. Access to Covered Account Information**

Access to covered account information shall be limited to employees that provide customer service and technical support for City departments or offices offering covered accounts. Any computer that has access to customer account or personal identifying information shall be password protected and all computer screens shall lock after no more than fifteen (15) minutes of inactivity. All paper and non-electronic based account or customer personal identifying information shall be stored and maintained in a locked room or cabinet, and access shall only be granted by the City Administrator or his/her designee.

**Section 1.1907. Credit Card Transactions**

All internet or telephone credit card payments shall only be processed through a third party service provider which certifies that it has an identity theft prevention program operating and in place. Credit card payments accepted in person shall require a reasonable connection between the person or entity billed for the services and the credit card owner.

**Section 1.1908. Suspicious Transactions**

Suspicious transactions include, but are not limited to, the presentation of incomplete applications, unsigned applications, payment by someone other than the person named on the covered account, or presentation of inconsistent signatures, addresses or identification.

Suspicious transactions shall not be processed and shall be immediately referred to the City Administrator or his/her designee.

**Section 1.1909. Notification of Law Enforcement**

The Compliance Officer or his/her designee shall use his/her discretion on whether to report suspicious transactions, to appropriate law enforcement departments

**Section 1.1910. Third Party Service Providers**

All transactions, processed through a third party service provider shall be permitted only if the service provider certifies that it has complied, with the FTC regulations and has in place a consumer identity theft prevention program.

**Section 1.1911. Compliance Officer and Training**

The Compliance Officer for this Identity Theft Prevention Program shall be the City Administrator or his/her designee. The City Administrator shall conduct training of all City employees that transact business using covered accounts. The City Administrator shall periodically review this program and recommend any necessary updates to the City Council.

**Section 1.1912. Annual Report**

The City Administrator shall provide an annual report to the Mayor. The contents of the annual report shall address and evaluate at least the following:

- 1) The effectiveness of the policies and procedures of the City in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to access to existing covered accounts;
- 2) Service provider arrangements;
- 3) Incidents involving identity theft with covered accounts and the City's response;
- 4) Changes in methods of identity theft and the prevention of identity theft; and
- 5) Recommendations for changes to the City's Identity Theft Prevention Program.

**SECTION 2. RECITALS**

The City Council hereby finds and declares all precatory language herein to be true and correct and approves and adopts the same herein as part of this Resolution.

**SECTION 3. SEVERABILITY**

If for any reason any section, paragraph, subdivision, clause, phrase or provision of this Ordinance shall be held invalid, it shall not affect any valid provisions of this or any other Ordinance of the City of Willow Park to which these rules and regulations relate.

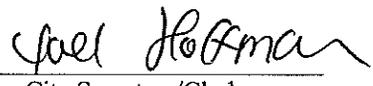
SECTION 4. EFFECTIVE DATE

This Ordinance shall take effect from and after the date of its adoption.

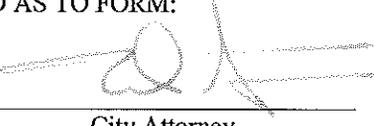
PASSED AND ADOPTED this 17<sup>th</sup> day of May, 2010.

/s/   
Mayor

ATTEST:

/s/   
City Secretary/Clerk

APPROVED AS TO FORM:

/s/   
City Attorney

The Willow Park City Council in acting on Ordinance No. 617-10 did on the 17<sup>th</sup> day of May, 2010, vote as follows:

	<u>FOR</u>	<u>AGAINST</u>
Kenneth Hawkins, Mayor	_____	_____
Barry K. Tatum, Place 1	<u>✓</u> _____	_____
Gene Martin, Place 2	<u>✓</u> _____	_____
Barry Brown, Place 3	<u>✓</u> _____	_____
Mark Hickerson, Place 4	<u>✓</u> _____	_____
Hale Alderman, Place 5	<u>✓</u> _____	_____