

Town of Friday Harbor , WA
IDENTITY THEFT PREVENTION PROGRAM

Findings

The Federal Trade Commission (“FTC”) requires every utility, to implement an Identity Theft Prevention Program (“ITPP”). The FTC requirement and regulation is necessary because of Section 114 of the Fair and Accurate Credit Transactions Act (“FACT Act”). The FTC has set forth the ITPP requirement in 16 C.F.R. § 681.2. Identity theft is defined as a fraud committed or attempted using identifying information of another person without authority. The Town of Friday Harbor adopts the program set forth in this Section to comply with FTC rules and regulations. In drafting its ITPP, the Town has 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 governing authority of the Town hereby determines that the Town is a low to moderate risk entity and as a result develops and implements the streamlined ITPP set forth in this Section. Further, the Town determines that the only covered accounts offered by the Town are those under its utilities.

Red Flags

The FTC regulations identify numerous red flags that must be considered in adopting an ITPP. The FTC has defined a red flag as a pattern, practice, or specific activity that indicates the possible existence of identity theft. The Town identifies the following red flags from the examples provided in the regulations of the FTC:

(1) Notifications from Consumer Reporting Agencies. The Town does not request, receive, obtain or maintain information about its utility customers from any Consumer Reporting Agency.

(2) Suspicious documents. Possible red flags include:

- i) presentation of documents appearing to be altered or forged;
- ii) presentation of photographs or physical descriptions that are not consistent with the appearance
- iii) of the applicant or customer;
- iv) presentation of other documentation that is not consistent with the information provided when
- v) the account was opened or existing customer information;
- vi) presentation of information that is not consistent with the account application; or
- vii) presentation of an application that appears to have been altered, forged, destroyed, or reassembled.

(3) Suspicious personal identifying information. Possible red flags include:

- i) 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 customer’s account application;
- ii) personal identifying information is associated with known fraudulent activity;
- iii) the social security number (if required or obtained) is the same as that submitted by another customer;
- iv) the telephone number or address is the same as that submitted by another customer;

- v) the applicant failed to provide all personal identifying information requested on the application; or
- vi) the applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

(4) Unusual use of or suspicious activity related to an account. Possible red flags include:

- i) a change of address for an account followed by a request to change the account holder's name;
- ii) a change of address for an account followed by a request to add new or additional authorized users or representatives;
- iii) 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);
- iv) 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);
- v) mail sent to the account holder is repeatedly returned as undeliverable;
- vi) the Town receives notice that a customer is not receiving his paper statements; or
- vii) the Town receives notice of unauthorized activity on the account.

(5) Notice regarding possible identity theft. Possible red flags include:

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

Proof of Ownership.

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

Confidentiality of Applications and Account Information.

All personal information, personal identifying information, account applications and account information collected and maintained by the Town shall be a confidential record of the Town and shall not be subject to disclosure unless otherwise required by State or Federal Law. Additionally, any employee with access to utility customers' personal information, account applications or account information shall be required to execute and abide by the Confidentiality and Nondisclosure Policy of the Town.

Access to Utility Account Information.

Access to utility account information shall be limited to employees that provide customer service and technical support to the Town's utilities. Any computer that has access to utility 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 utility 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 Compliance Officer or his/her designee.

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 utility services and the credit card owner.

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 utility account; presentation of inconsistent signatures, addresses or identification. Suspicious transactions shall not be processed and shall be immediately referred to the Compliance Officer or his/her designee.

Notification of Law Enforcement.

The Compliance Officer or his/her designee shall use his/her discretion on whether to report suspicious transactions to the police department or other appropriate law enforcement.

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.

Compliance Officer and Training.

The Compliance Officer for this ITPP and Section shall be the Town finance officer or his/her designee. The Compliance Officer shall conduct training of all Town employees that transact business with customers of the Town's utilities. The Compliance Officer shall periodically review this program and recommend any necessary updates to the Town Council.

Annual Report.

An annual report, as required by FTC regulations, shall be provided by the Compliance Officer to the Town Administrator. The contents of the annual report shall address and/or evaluate at least the following:

- (i) the effectiveness of the policies and procedures of the Town in addressing the risk of identity theft in connection with the opening of utility accounts and with respect to access to existing utility accounts;
- (ii) service provider arrangements;
- (iii) incidents involving identity theft with utility accounts and the Town's response;
- (iv) changes in methods of identity theft and the prevention of identity theft; and
- (v) recommendations for changes to the Town's ITPP.

RESOLUTION NO. 1681

A RESOLUTION by the Council of the Town of Friday Harbor adopting an Identity Theft Prevention Program.

WHEREAS, the Town of Friday Harbor provides utility service to its citizens; and

WHEREAS, The Fair and Accurate Credit Transactions Act of 2003, Pub. L. 108-159, (“Red Flags Rule”) requires certain financial institutions and 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; and

WHEREAS, the Town of Friday Harbor maintains certain continuing accounts with utility service 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, to comply with the Red Flags Rule, the Town has prepared an identity theft prevention program in the form attached hereto as Exhibit “A” and incorporated herein by this reference the “ITPP” or the program;

NOW, THEREFORE, BE IT RESOLVED by the Council of the Town of Friday Harbor that the Program is hereby approved and adopted effective the date set forth below and that the Town of Friday Harbor staff is hereby authorized and directed to implement the Program in accordance with its terms.

ADOPTED this 6th day of November 2008.

TOWN OF FRIDAY HARBOR

David F. Jones, Mayor

SEAL of the
Town of Friday Harbor
ATTEST:

Amy E. Taylor, Town Clerk