TOWN OF JOHNSTOWN
IDENTITY THEFT PREVENTION PROGRAM

PROGRAM ADOPTION

The Town of Johnstown ("Town") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements obligations imposed by the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. §§ 1681-1681x. This Program was developed with the oversight and approval of the Town's Finance Director. After consideration of the size and complexity of the Town's operations and account systems and the nature and scope of the Town's activities, the Town Council determined that this Program is appropriate for the Town, and therefore approved this Program by the adoption of Resolution No. 2021-03 on the 20th day of January, 2021.

PROGRAM PURPOSE AND DEFINITIONS

1. Fulfilling Requirements of the Red Flags Rule.

Pursuant to the Rule, every creditor is required to establish an identity theft prevention program tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

a. Identify relevant red flags as defined in the Rule and the program for new and existing covered accounts, and incorporate those red flags into a program;
b. Detect red flags that have been incorporated into the program;
c. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
d. Update the program periodically to reflect changes in risks to the customer or to the safety and soundness of the Town from identity theft.

2. Red Flags Rule Definitions Used in this Program

a. *Account* means a continuing relationship established by a person with a creditor to obtain a product or services for personal, family, household or business purposes.
b. *Covered Account* means
    i. Any account the Town offers or maintains primarily for personal or household purposes, that involves or is designed to permit multiple payments or transactions, such as utility accounts; and,
    ii. Any other account that the Town offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Town from identity theft.
c. *Creditor* has the same meaning as defined in Section 701 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a, and includes a person or entity that arranges for the extension, renewal or continuation of credit, including the Town.
d. *Customer* means a person or business entity that has a covered account with the Town.

e. *Identifying Information* means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, social security number, date of birth, official State or government issued identification number, alien registration number, government passport number, employer or taxpayer identification number or unique electronic identification number.
f. *Identity theft* means a fraud committed or attempted using identifying information of another person without authority.
g. *Person* means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative or association.
h. *Red Flag* means a pattern, practice or specific activity that indicates the possible existence of identity theft.
i. *Service Provider* means a person or business entity that provides a service directly to the Town relating to or in connection with a covered account.
j. *Town* means the Town of Johnstown.

3. Identification of Red Flags

In order to identify relevant red flags, the Town shall review and consider the types of covered accounts that it offers and maintains, the methods it provides to open covered accounts, the method it provides to access its covered accounts, and its previous experiences with identity theft. The Town identifies the following red flags, in each of the listed categories.

a. Notification and warnings from credit reporting agencies.
    i. Report of fraud accompanying a credit report;
    ii. Notice or report from a credit agency of a credit freeze on a customer or applicant;
    iii. Notice or report from a credit agency of an active-duty alert for an applicant; or
    iv. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.
b. Suspicious documents.
    i. Identification document or card that appears to be forged, altered or inauthentic;
    ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
    iii. Other document with information that is not consistent with the existing customer information (such as a signature on a check that appears forged; or
    iv. Application for service that appears to have been altered or forged or appears to have been destroyed and reassembled.
c. Suspicious personal identifying information.
    i. Identifying information presented that is inconsistent with other information the customer provides (such as inconsistent driver's license numbers);
    ii. Identifying information presented that is inconsistent with other sources of information (for instance, an address that does not match an address on the driver's license);

iii. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
iv. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
v. Social security number presented that is the same as one given by another customer;
vi. An address or telephone number presented that is the same as that of another person;
vii. Failing to provide complete personal identifying information on an application when reminded to do so;
viii. Identifying information which is not consistent with the information that is on file for the customer; or
ix. Inability to provide authenticating information beyond that which generally would be available from a wallet or consumer report.

d. Suspicious account activity or unusual use of account.
i. Change of address for an account followed by a request to change the account holder's name or the addition of authorized users on the account;
ii. Payments stop on an otherwise consistently up to date account;
iii. Account used in a way that is inconsistent with prior use;
iv. Mail sent to the account holder that is repeatedly returned as undeliverable;
v. Notice to the Town that a customer is not receiving mail sent by the Town;
vi. Notice to the Town that an account has unauthorized activity;
vii. Breach in the Town's computer system security; or
viii. Unauthorized access to or use of customer account information.

e. Alerts from others.
i. Notice to the Town from a customer, a victim of identity theft, a law enforcement authority or other person regarding the existence of a fraudulent account opened or maintained for a person engaged in identity theft.

4. <u>Detecting Red Flags</u>

In other to detect the red flags identified above associated with Town accounts, the Town shall implement the following procedures.

a. New Accounts: When a customer applies to open a new account, Town personnel shall take the following steps to obtain and verify the identity of the person opening the account:
i. Require certain identifying information such as name, address, principal place of business for an entity, driver's license or other identification;
ii. Verify the customer's identity (for instance, review driver's license or other form of government issued identification);
iii. Verify new resident status:
1. Homeowner: Require documented proof of sale from the seller or buyer; or

2. Renter: Require property owner consent before adding renter to account;

iv. Review documentation showing the existence of a business entity; and/or

v. Independently contact the customer.

b. Existing Accounts: In order to detect any red flags identified above for an existing account, Town personnel shall take the following steps to monitor transactions on an account:

i. Verify identification of customers if a person requests information whether that be in person, via telephone or email;

ii. Verify the validity of requests to change billing addresses; and/or

iii. Verify changes in banking information given for billing or payment purposes.

5. Preventing and Mitigating Identity Theft

In the event that the Town personnel detect any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the red flag:

a. Prevent and Mitigate Identity Theft.

i. Contact the customer with the covered account;

ii. Request additional identifying information from the applicant;

iii. Change any passwords or other security codes and devices that permit access to a covered account;

iv. Not open a new account;

v. Close an existing covered account;

vi. Not attempt to collect payment on a covered account;

vii. Notify the Finance Director for a determination of the appropriate steps to take;

viii. Notify law enforcement; and/or

ix. Determine that no response is warranted under the particular circumstances.

b. Protect Customer Identifying Information.

In order to further prevent the likelihood of identity theft occurring with respect to Town accounts, the Town shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

i. Limit access to personal identifying information to those employees responsible for or otherwise involved in opening covered accounts or accepting payment on a covered account;

ii. Input payment information provided to Town employees for a covered account directly into the Town's computer system without otherwise recording such information;

iii. Ensure Town computers are password protected and locked after a set period of time;

iv. Mask credit card numbers except for the last four digits;

v. Permit only limited staff to change customer accounts and records, with all other staff having view only access; and

vi. Undertake complete and secure destruction of paper documents and computer files containing customer information.

6. Program Administration

a. Oversight.
The Finance Director shall be responsible for developing, implementing and updating the Program. Any recommended material changes to the Program shall be submitted to the Town Council for consideration.

b. Staff Training.
Town staff responsible for implementing the Program shall be trained either by or under the direction of the Finance Director in the detection of red flags, and the responsive steps to be taken when a red flag is detected. Additionally, a compliance report shall be provided annually by the Finance Director to the Town Manager. The annual compliance report shall at a minimum address the following:
    1. The probable effectiveness of the Town's policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
    2. Service provider arrangements;
    3. Significant incidents involving identity theft and the Town's response; and
    4. Recommendations for material changes to the Program.

c. Service Provider Arrangements.
In the event that the Town engages a service provider to perform an activity in connection with one or more covered accounts, the Town shall take the following steps to require that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.
    1. Require by contract that service providers acknowledge receipt and review of the Program and agree to perform their activities with respect to Town covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Finance Director relative to the Program; or
    2. Require by contract that service providers acknowledge receipt and review of the Program and agree to perform their activities with respect to Town covered accounts in compliance with the terms and conditions of the service provider's identity theft program and tol take appropriate action to prevent and mitigate identity theft; and
    3. Require by contract that service providers agree to report promptly to the Town in writing if the service provider in connection with a Town covered account detects an incident of actual or attempted identity theft or is unable to resolve one or more red flags that the service provider detects in connection with a covered account.

d. Customer Identifying Information and Public Disclosure

The identifying information of Town customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law.

7. Program Updates

The Program shall be periodically reviewed and updated to reflect changes in risks to customers and to the safety and soundness of the Town from identity theft. The Finance Director shall at least annually consider the Town's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in the types of accounts that the Town maintains and changes in the Town's business arrangements with other entities and service providers. After consideration of these factors, the Finance Director shall determine if changes to the Program are warranted. If warranted, any material changes shall be brought to the Town Council for consideration.