

**CITY OF NORTH ROYALTON
IDENTITY THEFT PREVENTION PROGRAM
FOR
THE DEPARTMENT OF WASTE WATER TREATMENT**

The City of North Royalton (“City”) has approved and adopted this Identity Theft Prevention Program (“Program”). This Program has been developed in accordance with the Federal Trade Commission’s Identity Theft Prevention Red Flag Rules (16 CFR § 681.2). This Program has been created after conducting an assessment of the risk of Identity Theft associated with certain accounts that arise as a result of providing waste water treatment to properties within the City.

I. Definitions

For purposes of the Program, the following terms are defined as:

- A. “Consumer” means the holder of a Covered Account.
- B. “Covered Account” means (i) any account that the City offers or maintains primarily for personal family or household purposes which involves multiple payments or transactions or one or more deferred payments and (ii) any other account the City identifies as having a reasonably foreseeable risk to customers. The City has identified Covered Accounts for purposes of this Program as being all accounts for which the City provides waste water treatment and bills the Consumer periodically at a time subsequent to said services.
- C. “Department Billing Personnel” means any employee of the City that work with, or is responsible for, the billing for services provided by the Department of Waste Water Treatment.
- D. “Identity Theft” means fraud committed using the identifying information of another person.
- E. “Red Flags” mean a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

II. Program Purposes

The purposes of the Program are to:

- 1) Identify the relevant Red Flags based on the risk factors associated with the City’s Covered Accounts;
- 2) Institute policies and procedures for detecting Red Flags;
- 3) Identify steps the City, its administration, and/or outside service providers will take to prevent and mitigate Identity Theft; and
- 4) Create a system for regular updates and administrative oversight of the Program.

III. Identification of Red Flags

Red Flags generally fall within one of the following four general categories:

- 1) Suspicious documents;
- 2) Suspicious personal identifying information;
- 3) Suspicious or unusual use of a Covered Account; and
- 4) Alerts from others (e.g. customer, Identity Theft victim, or law enforcement).

“Column A” of the attached Appendix A is a list of some Red Flags that would be most relevant to the City for purposes of the services provided by the City’s Department of Waste Water Treatment.

IV. Detection of Red Flags

- A. Creation of Accounts
 - 1. This Program recognizes that the City creates Covered Accounts with Consumer information provided to the City by the City of Cleveland Division

of Water. The City does not create Covered Accounts based upon any direct interaction, written or oral, with Consumers.

2. The City of Cleveland Division of Water provides the City with the following information in order to create a Covered Account:
 - a) Name of Consumer;
 - b) Address of property serviced by the account;
 - c) Mailing address of account holder; and
 - d) Division of Water account number.

B. Detecting Red Flags

1. Because Department Billing Personnel create accounts solely from the information provided by the City of Cleveland Division of Water, Red Flags will most likely arise, if ever, from information obtained, or communications received, by the Department Billing Personnel after the Covered Account has been opened. When Department Billing Personnel become aware of any Red Flags, including those set forth in “Column A” of the attached Appendix A, they shall follow the procedures set forth below in this Program policy.
2. Notwithstanding the foregoing, when a Covered Account is opened and the billing address is different than the address of the property which is serviced by the utility, Department Billing Personnel shall notify the individual or business at the billing address that such account has been opened and that the address is being used for billing purposes. Such notification may be accomplished by written correspondence or by verbal communications.

V. Preventing and Mitigating Identity Theft

- A. When a Red Flag arises, Department Billing Personnel will take appropriate steps to investigate the Red Flag to determine if there is credible evidence of Identity Theft. Such steps are set forth in “Column B” of the attached Appendix A.
- B. If credible evidence of Identity Theft is found, the Director of Finance shall be notified of the situation immediately by Department Billing Personnel. The Director of Finance shall instruct on the appropriate steps to prevent the continuation of the Identity Theft and to mitigate damages arising from the Identity Theft. Such steps may include:
 - 1) Informing the individual whose identity has been used and assisting that individual in taking actions to mitigate damage from the Identity Theft, such as providing information to third parties, if requested to do so by the individual.
 - 2) Stop billing and collections actions against the Identity Theft victim.
 - 3) Notify law enforcement.
 - 4) Any other action deemed appropriate by the Director of Finance or Mayor.

C. Future Outside Service Providers

1. On the effective date of this Program, the City does not use an outside service provider (“Service Provider”) for Consumer billing, except for printing and mailing services.
 - a. With respect to printing and mailing services, the City shall ensure that the Service Provider has a policy in place to prevent theft of the personal identifying information contained on the City’s invoices for its Covered Accounts which are in the possession of the Service Provider.
2. If the City decides to use Service Provider for Consumer billing after the adoption of this Program, the City will require each Service Provider to implement its own Identity Theft prevention policy in accordance with the FTC’s Red Flag Rules. The City will review the Service Provider’s policy and will require changes to said policy, as it pertains to the City’s billing accounts, when needed.

3. The Service Provider’s policy shall include the following provisions:
 - a.) That all Red Flags be responded to in accordance with the Service Provider’s Identity Theft prevention policy.
 - b.) That all Red Flags which are not reconciled upon initial review by the Service Provider staff shall be escalated to supervisory staff for further investigation.
 - c.) That when there is verification of a Red Flag by the supervisory staff, and it appears that there is credible evidence that Identity Theft has occurred, the Service Provider shall inform the City of such in writing and take action on the account only in accordance with the City’s direction.
4. The City will designate a supervisory level employee in the City’s Administration to be responsible for coordinating with the Service Provider and other City employees and officials on possible Identity Theft situations.

VI. Program Administration and Training

The City Director of Finance, with the assistance of the Director of Law, is responsible for developing, implementing, administering and updating the Program. The Director of Finance, or his/her designee, will be responsible for developing a training program for Department Billing Personnel and any other City employee identified by the Director of Finance as having a role in implementing the Program. Training on this Program shall occur upon hiring of Department Billing Personnel and on an “as needed” basis thereafter. A record of training shall be kept by the Director of Finance.

VII. Updating of Program

The Director of Finance will periodically review the effectiveness of the Program and update the Program to reflect the addition or removal of Covered Accounts and changes in risks to Consumers from Identity Theft. An annual report shall be provided by the Director of Finance to the Mayor regarding significant incidents involving Red Flags and the City’s response, the effectiveness of the Program, and recommendations for change.

Signed into effect by:

Mayor Robert A. Stefanik

Date: _____

Adopted by City Council through Resolution No. _____

Passed _____

Acknowledged by:

Director of Finance

Date: _____

Appendix A

EXAMPLES OF IDENTITY THEFT RED FLAGS (Column A)	PREVENTION/MITIGATION PROCEDURES (Column B)
Documents provided for identification appear to have been altered or forged.	Require account holder to provide additional satisfactory information to verify identity.
Complaint/inquiry from an individual based on receipt of a notice of service, a bill, or a delinquency notice for a property that is not owned, used, or under the responsibility of the individual.	Stop the billing process and investigate discrepancy.
Complaint/inquiry from an individual about information added to a credit report for utility services.	Stop the billing process and investigate discrepancy.
Complaint/inquiry from an individual about a lien placed upon his/her property for delinquent utility services.	Stop the billing process and investigate discrepancy.
Mail sent to the account holder address is returned repeatedly as undeliverable although account holder insists on using the address in connection with the account.	Investigate discrepancy.
Utility provider is notified of an identity theft by a Consumer, a victim of identity theft, a law enforcement authority, or any other person that has opened a fraudulent account for a person engaged in identity theft.	Stop billing on account and attempt to identify proper party on the account; cooperate with the victim.