

**Policy: Identity Theft–FACTA Compliance  
Red Flags**

Adopted: M2009-xxx

Effective: 10/30/09

Revised:

**Purpose** The purpose of the program is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

**Policy** The risk to the City of Northfield, its employees and customers from data loss and identity theft is of significant concern to the City of Northfield and can be reduced only through the combined efforts of every employee and contractor. This policy enables the City of Northfield to protect existing customers, reduce risk from identity fraud, and minimize potential damage to the City of Northfield from fraudulent new accounts. The City of Northfield adopts this sensitive information policy to help protect employees, customers, contractors, and the city from damages related to the loss or misuse of sensitive information.

**Sensitive Data** Sensitive information:

- Credit card information including credit card number, credit card expiration date, cardholder name, and cardholder address.
- Tax identification numbers, including social security number, business identification number and employer identification numbers.
- Payroll information including paychecks and pay stubs.
- Medical information for any employee or customer including but not limited to doctor names, claims, insurance claims, prescriptions, and any other related personal medical information.
- Other personal information belonging to any customer, employee or contractor, including date of birth, address, phone numbers, maiden name, names and customer number.

**MGDPA** City personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this policy should be read in conjunction with the Minnesota Government Data Practices Act (MGDPA) Chapter 13. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor. In the event that the city cannot resolve a conflict between this policy and the Minnesota Government Data Practices Act, the city will contact the Commissioner of Administration for an advisory opinion.

**Hard Copy Distribution** Each employee and contractor performing work for the city will comply with the following:

- File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
- Storage rooms containing documents with sensitive information and records retention areas will be locked at the end of each workday or when unsupervised.

**Policy: Identity Theft–FACTA Compliance  
Red Flags**

Adopted: M2009-xxx

Effective: 10/30/09

Revised:

- ❑ Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
- ❑ Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
- ❑ When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled “Confidential paper shredding and recycling. City records, however, may only be destroyed in accordance with the city’s records retention policy.

**Electronic  
Distribution**

Each employee and contractor performing work for the city will comply with the following:

- ❑ Internally, sensitive information may be transmitted using approved city e-mail. All sensitive information must be encrypted when storing in an electronic format.
- ❑ Any sensitive information sent externally must be encrypted and password protected and only sent to approved recipients. Additionally, a statement such as what follows should be included in the e-mail:

*“This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited.”*

**Covered Accounts**

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by identity theft.

- ❑ Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft;
- ❑ Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the city from identity theft, including financial, operations, compliance, reputations, or litigation risks.

**Policy: Identity Theft–FACTA Compliance  
Red Flags**

Adopted: M2009-xxx

Effective: 10/30/09

Revised:

**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.

- Alerts, notifications or warnings from a consumer reporting agency;
- A fraud or active duty alert included with a consumer report;
- A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report as defined in § 334.82 (b) of the Fairness and Accuracy in Credit Transactions Act.
- Consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer.
- A recent and significant increase in the volume of inquiries.
- An unusual number of recently established credit relationships.
- A material change in the use of credit, especially with respect to recently established credit relationships
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
- Documents provided for identification that appears to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the city, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- Personal identifying information provided is inconsistent when compared against external information sources used by the city.
- The address does not match any address in the consumer report.
- The Social Security number (SSN) has not been issued or is listed on the Social Security Administration’s Death Master File
- Personal identifying information provided by the customer is not consistent with other personal identifying information by the customer,
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third party sources used by the city.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or their-party sources used by the city.
- The address on an application is fictitious, a mail drop, or a prison
- The phone number is invalid or is associated with a pager or answering service.
- The social security number provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the

**Policy: Identity Theft–FACTA Compliance  
Red Flags**

Adopted: M2009-xxx

Effective: 10/30/09

Revised:

address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.

- The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the city.
- When using security questions (mother's maiden name, pet's name, etc.) the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- Shortly following the notice of a change of address for a covered account, the city receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account. Such as nonpayment when there is no history of late or missed payments or a material change in purchasing or usage patterns.
- A covered account that has been inactive for a reasonably lengthy period of time is used.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- The city is notified that the customer is not receiving paper account statements.
- The city is notified of unauthorized charges or transactions in connection with a customer's covered account.
- The city receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the city.
- The city is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

**Responding to Red  
Flags**

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the city from damages and loss.

- Gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.
- The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.
- Cancel the transaction
- Notify and cooperate with appropriate law enforcement
- Determine extent of liability of the City of Northfield. Notify the actual

**Policy: Identity Theft–FACTA Compliance  
Red Flags**

Adopted: M2009-xxx

Effective: 10/30/09

Revised:

customer that fraud has been attempted.

**Periodic Updates to Plan** At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

- Periodic reviews will include an assessment of which accounts are covered by the program.
- Red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.
- Actions to take in the even that fraudulent activity is discovered may also require revision to reduce damage to the city and its customers.

**Program Administration** Operational responsibility of the program is delegated to the City Administrator.

**Staff Training** Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contract with accounts or personally identifiable information that may constitute a risk to the city or its customers.

- Human Resources is responsible for ensuring identity theft training for all requisite employees and contractors.
- Employees must receive annual training in all elements of this policy.
- To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

**Oversight of service provider arrangements** It is the responsibility of the city to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

- A service provider that maintains its own identity theft prevention program consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
- Any specific requirements should be specifically addressed in the appropriate contract arrangements.