HISTORIC
FRANKLIN
TENNESSEE

Identity Theft Prevention Program
City of Franklin
Revision 1.0

1/11/2010

This document supersedes all previous identity theft prevention program documents.

Approved and Adopted by:
The Board of Mayor and Aldermen

Date:_____

Table of Contents

1 Introduction

Statement of Need and Definition

Customers depend on City of Franklin to properly protect personal, nonpublic information, which is gathered and stored in internal records. Regulatory agencies are charged with the responsibility to ensure financial institutions and creditors information security controls and procedures are in compliance with the intent of the regulations to protect a customer's identity. Therefore, it is important for management and staff to understand the basic security requirements and provide ongoing assistance in detection, prevention, and mitigation of identity theft to City of Franklin's customers.

Compliance

This Identity Theft Prevention Program is designed to emphasize compliance with all information security requirements, including those detailed in the regulatory agency guidelines. Specifically, the intent of the Identity Theft Prevention Program is to meet the objectives of the FACT Act, as set forth in FTC Rules and Regulations 16 CFR Part 681 – Identity Theft Red Flags. Furthermore, the Identity Theft Prevention Program is aligned with FFIEC and FTC requirements.

Objective

City of Franklin's objective is to develop a written Identity Theft Prevention Program, designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

- The Risk Manager of the City of Franklin will serve as the organization's Identity Theft Prevention Coordinator.
- The program will be updated periodically to reflect changes in risks to customers, vendors, employees, and to the safety and soundness of the City of Franklin from identity theft.

Goals

The specific goals of this program are to:

- Identify relevant Red Flags for the covered accounts that City of Franklin offers or maintains.
- Define reasonable policies and procedures to detect and respond to identified Red Flags.
- Update the program and Red Flags periodically to reflect changes in risks to customers, vendors, employees, and to the safety and soundness of City of Franklin.
- Ensure the Board of Mayor and Aldermen's involvement in the adoption of the organization's written Identity Theft Prevention Program and ongoing oversight of the integral parts of the Identity Theft Prevention Program and related Red Flags.
- Establish responsibility for implementation and maintenance of the Identity Theft Prevention Program, including ongoing review of Red Flags.
- Design, implement, and maintain information security controls to address identified risks relative to the sensitivity level of customer information.
- Train management and staff, as necessary, to effectively implement the Identity Theft Prevention Program.
- Exercise appropriate and effective oversight of service providers and require these vendors to provide appropriate measures designed to meet the control objectives of the Identity Theft Prevention Program.
- Report to the Board of Mayor and Aldermen at least annually. The report will address material matters related to the Program and evaluate issues such as: the effectiveness of 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; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

Responsibility

The responsibility of maintaining an effective Identity Theft Prevention Program is assigned to the FACTA Committee.

The FACTA Committee will be responsible for the appointment of an Identity Theft Prevention Coordinator. The current Identity Theft Prevention Coordinator will be the Risk Manager. The Identity Theft Prevention Coordinator will report to the City of Franklin City Administrator and the Board of Mayor and Aldermen.

Regulatory Requirement

16 CFR Part 681 (c) (Periodic Identification of Covered Accounts) states:

> "Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this determination, the City of Franklin must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:
>
> (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."

Purpose

The risk assessment required per 16 CFR Part 681 (c) determines if an institution has covered accounts and, consequently, must develop a formal Identity Theft Prevention Program. The risk assessment must be updated periodically based on changes in methods used to open accounts, methods available to access accounts and the institution's experience with identity theft.

Risk Factors

Based on City of Franklin's Identity Theft Prevention Program Risk Assessment, the following risk factors have been identified:

Types of covered accounts offered:

- Blue Cross Blue Shield Account
- Business Taxation Accounts
- Cigna-Disability Life Insurance Account
- City Court Accounts
- Delta Dental of Tennessee
- Employee Payroll Account
- Financial Background Investigations
- Fort Dearborn Life Insurance Company
- FSA Administrator
- HM Life Insurance Co.
- Life Insurance Company of North America
- Suntrust Account
- USABLE-Flex Benefits
- Utility Billing Account (opening)
- Vendor Accounts
- Website Payment Accounts

Methods to open a covered account:

- By Telephone
- In Person
- Over the Internet

- Through a Third Party
- Through the Mail

Methods to access a covered account:

- Automatic Transfers
- By Telephone
- In Person
- Over the Internet
- Through a Third Party
- Through the Mail

Threat and Risk Levels

The Identity Theft Risk Assessment follows a qualitative model. Risk levels are determined by considering the likelihood and potential damage of an event as defined below.

Likelihood definitions

- **Low:** Identity Theft is not expected, but there's a slight possibility it may occur at some time.
- **Medium:** Identity Theft might occur at some time based on a history of limited occurrence, type of covered account, and size and complexity of the organization.
- **High:** Identity Theft will probably occur based on a history of frequent occurrence, type of covered account, and size and complexity of the organization.

Damage Potential definitions

- **Minimal:** Identity Theft may result in the minor loss of some resources and reputation.
- **Moderate:** Identity Theft may result in loss of resources and reputation which could harm the organization's ability to achieve its mission.
- **Major:** Identity Theft may result in the loss of major resources and reputation which would harm the organization's ability to achieve its mission.

Risk Level definitions

- **Low:** Impact is minimal and could even be considered a cost of doing business.
- **Medium:** Impact could be significant and possibly affect the stability of the organization.
- **High:** Impact is major and could threaten the stability of the organization.

Conclusion

Based on the Identity Theft Prevention Program Risk Assessment, City of Franklin has confirmed it is required to develop and maintain an Identity Theft Prevention Program.

2.1 Risk Matrix

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Blue Cross Blue Shield Account	Opened Fraudulently	In Person	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Medium	Minimal	Medium
Business Taxation Accounts	Opened Fraudulently	In Person, Over the Internet, Through the Mail	Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	None	None	N/A	N/A	N/A
Cigna-Disability Life Insurance Account	Opened Fraudulently	In Person, Over the Internet, Through a Third Party, Through the Mail	Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	Automatic Transfers, By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low
City Court Accounts	Opened Fraudulently	In Person	Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	Automatic Transfers, By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Delta Dental of Tennessee	Opened Fraudulently	In Person	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Employee Payroll Account	Opened Fraudulently	In Person, Through a Third Party	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	Automatic Transfers, By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Moderate	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Financial Background Investigations	Opened Fraudulently	By Telephone, In Person, Over the Internet, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Fort Dearborn Life Insurance Company	Opened Fraudulently	In Person, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
FSA Administrator	Opened Fraudulently	In Person, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
HM Life Insurance Co.	Opened Fraudulently	In Person	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Life Insurance Company of North America	Opened Fraudulently	In Person, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Suntrust Account	Opened Fraudulently	Over the Internet	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Moderate	Low
	Unauthorized Access	Automatic Transfers, By Telephone, Over the Internet, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
USABLE-Flex Benefits	Opened Fraudulently	In Person, Over the Internet, Through the Mail	Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Utility Billing Account (opening)	Opened Fraudulently	In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	By Telephone, In Person, Over the Internet, Through a Third Party, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Vendor Accounts	Opened Fraudulently	In Person, Over the Internet, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	Automatic Transfers, By Telephone, In Person, Over the Internet, Through the Mail	Customer is Not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low
Website Payment Accounts	Opened Fraudulently	Over the Internet	Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

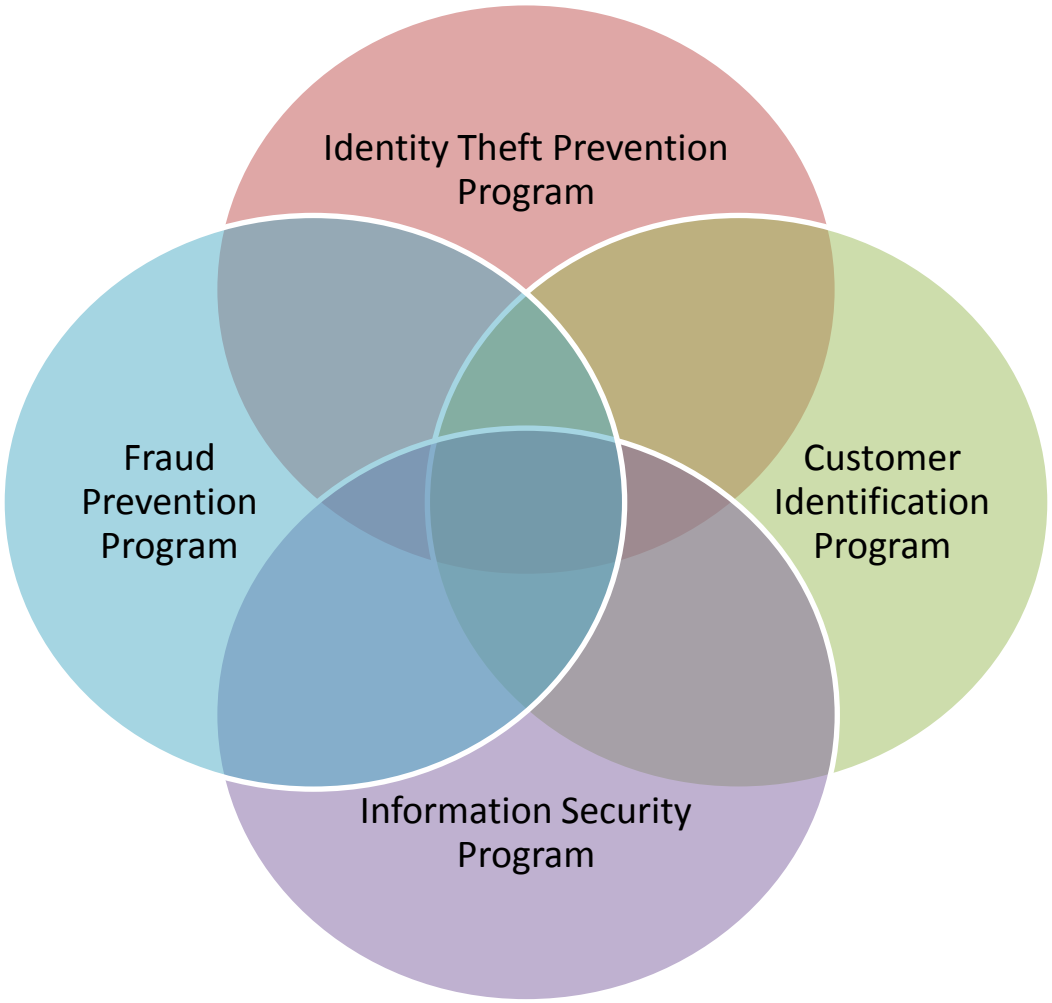
Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
	Unauthorized Access	Automatic Transfers, Over the Internet	Account Use is Inconsistent with Normal Activity, Address or Telephone Number Flags, An Attempted Reopening of an Internally Terminated Account, Application Appears to be Altered or Forged, Documents Altered or Forged, Fraudulent Web Site, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail or Email is Returned on an Active Account, New Covered Account Follows Fraud Patterns, Notice that a Fraudulent Account Has Been Opened, Notification of Unauthorized Charges or Transactions, The SSN Has Been Submitted by Other Persons, Unusual Activity Pattern on Covered Account or Applicants	Low	Minimal	Low

Statement

The Board of Mayor and Aldermen of the City of Franklin requires the organization to develop and implement a comprehensive Identity Theft Prevention Program, which identifies relevant Red Flags for all covered accounts. The program will be reviewed and assessed on an annual basis, and the results will be reported to the Board of Directors.

The following other Programs relate to the Identity Theft Prevention Program:

- The Customer Identification Program per 31 U.S.C. 5318(l) (31 CFR 103.121)
- The Fraud Prevention Program
- The Information Security Program: including Information Security Risk Assessment, and Information Security Policies per Gramm-Leach-Bliley Act (GLBA)



3.1 Identification of Relevant Red Flags

Risk Factors

To identify relevant Red Flags, City of Franklin has evaluated the following factors (see Risk Assessment section above):

Types of covered accounts:

City of Franklin offers the following types of covered accounts:

- Blue Cross Blue Shield Account
- Business Taxation Accounts
- Cigna-Disability Life Insurance Account
- City Court Accounts
- Delta Dental of Tennessee
- Employee Payroll Account
- Financial Background Investigations
- Fort Dearborn Life Insurance Company
- FSA Administrator
- HM Life Insurance Co.
- Life Insurance Company of North America
- Suntrust Account
- USABLE-Flex Benefits
- Utility Billing Account (opening)
- Vendor Accounts
- Website Payment Accounts

Methods to open a covered account:

- By Telephone
- In Person
- Over the Internet
- Through a Third Party
- Through the Mail

Methods to access a covered account:

- Automatic Transfers
- By Telephone
- In Person
- Over the Internet
- Through a Third Party
- Through the Mail

Previous experiences with identity theft:

City of Franklin will take into account previous experiences with identity theft when defining and updating Red Flags.

Sources of Red Flags

City of Franklin will incorporate relevant Red Flags from sources such as:

- Incidents of identity theft City of Franklin has experienced.
- Methods of identity theft that reflect changes in identity theft risks.

- Applicable supervisory guidance.

Categories of Red Flags

City of Franklin will categorize relevant Red Flags into the following categories:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
- The presentation of suspicious documents.
- The presentation of suspicious personal identifying information, such as a suspicious address change.
- The unusual use of, or other suspicious activity related to, a covered account.
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identify theft in connection with covered accounts held by the financial institution or creditor.

See Section 3 (Red Flags) for a list of identified, relevant Red Flags.

3.2 Detection of Red Flags

Detecting Red Flags

City of Franklin will address detection of Red Flags in connection with opening of covered accounts and existing covered accounts by:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account. City of Franklin will use the policies and procedures regarding identification and verification set forth in the Customer Information Program (CIP), as defined in 31 U.S.C. 5318(l) (31 CFR 103.121).
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

3.3 Prevention and Mitigation of Identity Theft

Preventing and Mitigating Red Flags

City of Franklin has measures in place to appropriately respond to Red Flags detected that are commensurate with the degree of risk posed. Appropriate responses may include:

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances..

When determining the appropriate response, City of Franklin will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the City of Franklin or a third party, or notice that a customer has provided information related to a covered account held by City of Franklin to someone fraudulently claiming to represent City of Franklin or to a fraudulent website.

3.4 Update the Program

Updating the Program

City of Franklin will update the Program (including a review of relevant Red Flags) periodically, to reflect changes in risks to customers or to the safety and soundness of City of Franklin from identity theft based on factors such as:

- The experiences of City of Franklin with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that City of Franklin offers or maintains.
- Changes in the business arrangements of City of Franklin including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

3.5 Administration of the Program

Oversight of the Program

The responsibility of maintaining an effective Identity Theft Prevention Program is assigned to the FACTA Committee.

The FACTA Committee will be responsible for the appointment of an Identity Theft Prevention Coordinator. The current Identity Theft Prevention Coordinator will be the Risk Manager. The Identity Theft Prevention Coordinator will report to the FACTA Committee.

The Identity Theft Prevention Coordinator will:

- Work closely with the organization's senior management and front line personnel to identify, detect, and respond to appropriate Red Flags,
- Assign specific responsibility for the Program's implementation,
- Approve material changes to the Program as necessary to address changing identity theft risks, and
- Report to the Board of Mayor and Aldermen at least annually on the compliance of the Program. The report should address material matters related to the Program and evaluate issues such as:
  - The effectiveness of the policies and procedures of City of Franklin in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts,
  - Service provider arrangements,
  - Significant incidents involving identity theft and management's response, and
  - Recommendations for material changes to the Program.

Oversight of Service Providers

Whenever City of Franklin engages a service provider to perform an activity in connection with one or more covered accounts, City of Franklin will take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, City of Franklin might require the service provider by contract to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to City of Franklin or take appropriate steps to prevent or mitigate identity theft.

Staff Training

The City of Franklin will educate employees to identify and respond to Red Flags. Training supports security awareness and strengthens compliance with the Identity Theft Prevention Program. Ultimately, the behavior and priorities of senior management heavily influence the level of employee awareness and policy compliance, so training and the commitment to security starts with senior management.

Staff will be trained as necessary to effectively implement the Program. Training materials for City of Franklin will review the identification, detection and response to Red Flags.

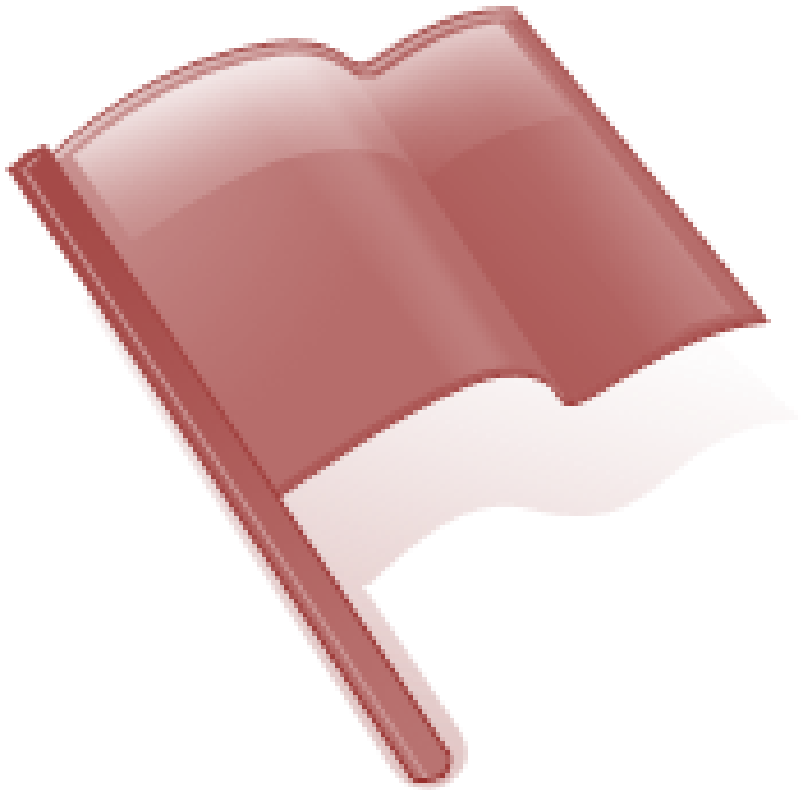
3.6 Other Applicable Legal Requirements

City of Franklin will be mindful of other related legal requirements that may be applicable, such as:

- Filing a Suspicious Activity Report under 31 U.S.C. 5318 (g);
- Implementing requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the City of Franklin detects a fraud or active duty alert;
- Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and
- Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

4 Red Flag Policies and Procedures

The following Red Flag Policies and Procedures are designed to identify, detect, and respond appropriately to identity theft in connection with the opening of a covered account or access to an existing covered account.



4.1 Alerts, Notifications or Warnings

Red Flags associated alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.

4.1.1 Consumer Report Address Discrepancy

Red Flag

A consumer reporting agency provides a notice of address discrepancy.

Detection

A consumer report is run for all police officer applicants, all director applicants, assistant administrator applicants, and city administrator applicants . Consumer reports are reviewed by the background investigator, Chief of Police and Human Resources Director.

Response

Determine from the consumer or customer why the consumer report provided a notice of address discrepancy.

Confirm the address of the consumer or customer by:

- Verifying the customers address with the address City of Franklin has on file.
- Verifying the customers address through a third party.

Verification

Review procedures to run consumer reports on a regular basis.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.1.2 Consumer Report Alert

Red Flag

A fraud or active duty alert is included with a consumer report.

Detection

Fraud Alerts (Police Department and Human Resources): The City of Franklin uses Credit Reports for employment background investigations for Law Enforcement, City Administrator, City Assistant Administrators, and City Director positions.

A Fraud Alert is a statement in the Credit Report Agency (CRA) file of a consumer that:

1. Notified all prospective users of a consumer report relating to the consumer (City Applicant) that the consumer may be a victim of fraud, including identity theft; and

2. The Fraud Alert has been presented in a manner that facilitates a clear and obvious view of the statement described in the above paragraph by any person (Background Investigator) requesting the Credit Report shall use the following procedures.

Response

Determine from the consumer or applicant the reason for the alert. Upon receipt of an initial, extended or active duty alert, it is the responsibility of the assigned employee and/or department director designee to verify the identity of the applicant. If the alert contains instructions to contact the applicant before taking any action on the request, then the assigned employee must contact the applicant in the manner specified to verify identity.

If the employee is unable to confirm the identity, the department director or their designee shall deny approval to proceed with the background investigation, and make notification to the Director of Human Resources. Determination to continue the application process or notifying law enforcement will be made by the City Administrator, Director of Human Resources, and the Department Director.

If the employee is able to confirm the identity, the department director or their designee shall sign the form, allowing the employee to proceed with the background investigation.

Verification

Review procedures to run consumer reports on a regular basis.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.1.3 Consumer Report Credit Freeze

Red Flag

A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

Detection

A consumer report may be run a background investigator or human resources director. Consumer reports are reviewed by appropriate supervisory employee.

Response

Determine from the consumer or customer the reason for the credit freeze.

Record and document steps taken and final resolution.

Verification

Review procedures to run consumer reports on a regular basis. Ensure appropriate employees are trained to adequately review consumer reports.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director

4.1.4 Unusual Activity Pattern on Covered Account or Applicants

Red Flag

An employee, a customer, or a consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a customer or applicant, such as:

- 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

Detection

A consumer report may be run for a new police applicant, director applicant, assistant city administrator applicant, or city administrator applicant. Consumer reports are reviewed by appropriate supervisory employee.

Suspicious Activity. The unusual use of or other suspicious activity related to a customer account can be a Red Flag for identity theft. Suspicious activities may include:

(a) A customer fails to make the first payment or makes an initial payment but no subsequent payments on the account. A customer account is used in a manner which is not consistent with established patterns of use on the account such as:

(1) Nonpayment when there is no history of late or missed payments; or (2) A material change in the amount of utility service purchased; (c) Mail sent to the customer is returned repeatedly as undeliverable although utility purchases continue to be made on the customer account. (d) A request is made, by a person claiming to be a customer or by another person, for a customer's confidential information from the City's records.

4. Notices. Notices of potential identity theft are serious Red Flags may include:

(a) Notices from customers, law enforcement authorities or other persons indicating that a customer or other person may have been a victim of identity theft. (b) Notices to the City that a person has provided information to someone fraudulently claiming to represent the City. (c) Notices to the City that a fraudulent website which appears similar to the City's website is being used to solicit customer personal identifying information. (d) E-mails not initiated by the City, but returned on the City's mail servers , indicating that a customer may have received fraudulent e-mail soliciting customer personal identifying information.

Response

Determine from the applicant why the consumer report reflects a pattern of unusual activity. Determine from the customer why there is unusual activity with their account. If an employee or customer believes that an identity theft has occurred, report the theft to the Franklin Police Department immediately.

Verification

Review procedures to run consumer reports on a regular basis.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director

4.2 Suspicious Documents

Red Flags associated with the presentation of suspicious documents.

4.2.1 Application Appears to be Altered or Forged

Red Flag

An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled. Suspicious Documents. The presentation of suspicious documents can be a Red Flag for identity theft. Examples of suspicious documents may include the following:

(a) Documents provided for identification appear to have been altered or forged.(b) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification. c) Other information on the identification is not consistent with information provided by the person opening a new account or the customer presenting the identification.(d) Other information on the identification is not consistent with readily accessible information that is on file with the City, such as the customer's application for service.(e) An application for service appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

Detection

Prior to opening a new account, a customer is required to complete an application in person or online. The customer appears to provided forged or altered identification.

Notices from customers, law enforcement authorities or other persons indicating that a customer or other person may have been a victim of identity theft.

(b) Notices to the City that a person has provided information to someone fraudulently claiming to represent the City.

(c) Notices to the City that a fraudulent website which appears similar to the City's website is being used to solicit customer personal identifying information.

Response

Determine from the customer the reason for the appearance of the application. If necessary, require the customer to resubmit a new application.

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Verification

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.2.2 Documents Altered or Forged

Red Flag

Documents provided for identification appear to have been altered or forged.

Detection

Consumer and customer identity is verified prior to opening an account or making changes to an account (i.e. name or address change). Documents used to verify a customer's identity may include:

- For an individual - Unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
- For a person other than an individual (such as a corporation, partnership, or trust) - Documents establishing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or trust instrument.

See City of Franklin's Customer Identification Program for more details.

Response

Determine from the consumer or customer the reason for the appearance of the documents. If necessary, obtain verification of identity from the customer via other means.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.
- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director

4.2.3 Information on ID Inconsistent with Information on File

Red Flag

Other information on the identification is not consistent with readily accessible information that is on file with City of Franklin, such as billing information or an application.

Detection

Consumer and customer identity is verified prior to opening an account, or making changes to an account (i.e. address change). Documents used to verify a customer's identity may include:

- For an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
- For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as a certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.

See City of Franklin's Customer Identification Program for more details.

Response

Determine from the customer the reason for the inconsistency of their information. If necessary, obtain verification of identity from the customer via other means.

Take all appropriate reasonable steps to verify the customers identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, department director.

4.2.4 Information on ID Inconsistent with Information Provided

Red Flag

Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

Detection

The customer identity is verified prior to opening an account or making changes to an account (i.e. address change). Documents used to verify a customer's identity may include:

- For an individual - Unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
- For a person other than an individual (such as a corporation, partnership, or trust) - Documents establishing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or trust instrument.

See City of Franklin's Customer Identification Program for more details.

Response

Determine from the customer the reason for inconsistency of the information. If necessary, obtain verification of identity from the consumer or customer via other means.

Take all appropriate reasonable steps to verify the customer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.
- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.2.5 Photograph or Physical Description Inconsistency

Red Flag

The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

Detection

Consumer and customer identity is verified prior to opening an account or making changes to an account (i.e. name or address change). Documents used to verify a customer's identity may include:

- For an individual - Unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
- For a person other than an individual (such as a corporation, partnership, or trust) - Documents establishing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or trust instrument.

See City of Franklin's Customer Identification Program for more details.

Response

Determine from the consumer or customer the reason for the difference in photograph or physical description. If necessary, obtain verification of identity from the consumer or customer via other means.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor and the department director.

4.3 Suspicious Personal Identifying Information

Red Flags associated with the presentation of suspicious personal identifying information, such as suspicious address change.

4.3.1 Address or Telephone Number Flags

Red Flag

The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

Detection

Consumer and customer identity is verified through internal and third party resources prior to opening an account, or making changes to an account (i.e. address change).

See City of Franklin's Customer Identity Verification Program for procedures for verifying the identity of a customer.

Response

Determine from the customer the reason the address or telephone number is the same as one submitted by numerous other accounts. If necessary, obtain verification of identity from the customer via Veratad ID Plus. Other Responses could be:

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Verification

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.3.2 An Attempted Reopening of an Internally Terminated Account

Red Flag

An account was closed due to non-payment or abuse and there is an attempt to reopened the account in another parties name. There are discrepancies and inconsistency when trying to reopen the account.

- Name does not match the SSN
- SSN has multiple identities
- If business - Owner has an out of state drivers license

Detection

All account openings are monitored and must be customer must be verified prior to account opening.

Response

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree; OR:
- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Verification

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director

4.3.3 Challenge Question Responses Unavailable or Limited

Red Flag

For City departments that use challenge questions, 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.

Detection

Customer identity is verified prior to opening an account or making changes to an account (i.e. address change).

See City of Franklin's Customer Identification Program for procedures for verifying the identity of a customer.

Response

Determine the reason for the inconsistency. If necessary, obtain verification of identity from the customer via other means.

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Verification

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.3.4 Incomplete Application

Red Flag

The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

Detection

Prior to opening a new account, a customer is required to complete an application.

Response

Review the incomplete parts of the application. Determine from the customer why the application is incomplete. Require the customer to complete the required portions of the application.

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Verification

Ensure appropriate employees are trained to review applications.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.3.5 Personal ID Associated with Known Fraudulent Activity

Red Flag

Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- The address on an application is the same as the address provided on a fraudulent application;
- The phone number on an application is the same as the number provided on a fraudulent application;
- An account was closed for non-payment is being reopened by another party.

Detection

Consumer and customer identity is verified through internal and third party resources prior to opening an account or making changes to an account (i.e. address change).

See City of Franklin's Customer Identification Program for procedures for verifying the identity of a customer.

Response

Determine from the consumer or customer the reason the personal identifying information is associated with known fraudulent activity. If necessary, obtain verification of identity from the consumer or customer via other means.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor, and department director.

4.3.6 Personal ID is Inconsistent with External Information

Red Flag

Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

- 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.

Detection

Consumer and customer identity is verified through third party resources prior to opening an account, or making changes to an account (i.e. address change).

See City of Franklin's Customer Identification Program for procedures for verifying the identity of a customer.

Response

Determine from the consumer or customer the reason for the inconsistency. If necessary, obtain verification of identity from the consumer or customer via other means.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor, and department director.

4.3.7 Personal ID is Inconsistent with Information on File

Red Flag

Personal identifying information provided is not consistent with personal identifying information that is on file with the institution or creditor.

Detection

Consumer and customer identity is verified prior to opening an account or making changes to an account (i.e. name or address change).

See City of Franklin's Customer Identification Program for procedures for verifying the identity of a customer.

Response

Determine from the consumer or customer the reason for the inconsistency. If necessary, obtain verification of identity from the consumer or customer via other means.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor, and department director.

4.3.8 Personal ID is Inconsistent with Other Personal ID

Red Flag

Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

Detection

Consumer and customer identity is verified through internal and third party resources prior to opening an account, or making changes to an account (i.e. name or address change). The information is reviewed for discrepancies or inconsistencies.

See City of Franklin's Customer Identification Program for procedures for verifying the identity of a customer.

Response

Determine from the consumer or customer the reason for the inconsistency. If necessary, obtain verification of identity from the consumer or customer via other means.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor, and department director.

4.3.9 Personal ID is of a Type Common to Fraudulent Activity

Red Flag

Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the institution or creditor. For example:

- 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 SSN is unable to be verified
- The SSN is associated with another person(s)

Detection

Consumer and customer identity is verified through internal and third party resources prior to opening an account or making changes to an account (i.e. name and address change).

See City of Franklin's Customer Identification Program for procedures for verifying the identity of a customer.

Response

Determine from the consumer or customer the reason the information appears to be unusual. If necessary, obtain verification of identity from the consumer or customer via other means.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor, and department director.

4.3.10 The SSN Has Been Submitted by Other Persons

Red Flag

The SSN provided is the same as that submitted by other persons opening an account or other customers.

Detection

Consumer and customer identity is verified prior to opening an account, or making changes to an account (i.e. name or address change).

See City of Franklin's Customer Identification Program for procedures for verifying the identity of a customer.

Response

Verify with the customer the SSN they provided is correct. Determine from customer, why there are multiple individuals associated with SSN.

Take all appropriate reasonable steps to verify the consumer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See the City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.4 Unusual Use or Suspicious Activity

Red Flags associated with the unusual use of, or other suspicious activity related to, a covered account.

4.4.1 Account Use is Inconsistent with Normal Activity

Red Flag

A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- Nonpayment when there is no history of late or missed payments;
- A material change in electronic fund transfer patterns in connection with a deposit account;

Detection

City of Franklin monitors activity on revolving credit accounts for patterns of fraud or inconsistency.

Response

Ensure the identity of the customer. Determine from the customer the reason for the unusual pattern.

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Verification

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director

4.4.2 Customer is Not Receiving Account Statements

Red Flag

City of Franklin is notified that the customer is not receiving paper account statements.

Detection

The customer notifies City of Franklin they are not receiving paper account statements.

Response

Ensure the identity of the customer. Ensure the customer is configured to receive paper account statements. Verify the customers address and, if the address is different from the address on file, determine the reason for the change of address. If a change of address is required, follow appropriate procedures for a change of address.

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately respond to customer requests regarding address changes.

Responsibility

Identity Theft Prevention Coordinator

4.4.3 Inactive Account is Used

Red Flag

A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

Detection

Accounts are set to go inactive or dormant after a period of inactivity.

Response

Ensure the identity of the customer. Determine from the customer the reason for the account activity.

Verification

Ensure appropriate employees are trained to adequately review covered accounts.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director

4.4.4 Key Changes Shortly After Change of Address

Red Flag

Shortly following the notice of a change of address for a covered account, the City of Franklin receives a request for an addition of authorized users on the account.

Detection

City of Franklin verifies the identity of each customer prior to making key changes such as a request for a new or replacement cell or an addition of authorized users on an account.

Response

Determine from the customer the reason the changes. Ensure the identity of the customer through other means.

Take all appropriate reasonable steps to verify the customer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.
- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.4.5 Mail or Email is Returned on an Active Account

Red Flag

Mail or Email sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

Detection

City of Franklin will attempt to contact the customer with other means (i.e. phone, Email or alternate Email, SMS) to determine to reason for returned mail or Email.

Response

Ensure the identity of the customer. Determine from the customer the reason mail is being returned.

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Verification

Ensure appropriate employees are trained to address returned mail.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.4.6 New Covered Account Follows Fraud Patterns

Red Flag

A new covered account is used in a manner commonly associated with known patterns of fraud patterns. For example:

- The customer fails to make the first payment or makes an initial payment but no subsequent payments;
- An account which was closed for non-payment of abuse is reopened under a different name.

Detection

City of Franklin monitors activity on revolving credit accounts for patterns of fraud or inconsistency.

Response

Ensure the identity of the customer. Determine from the customer the reason for the unusual pattern. Verify customer using internal or external means.

Take all appropriate reasonable steps to verify the customer's identity and confirm the application to open the account was not the result of identity theft.

- These steps to verify should include a combination of the following - Validation (through a 3rd party or otherwise) of name, address, date of birth, SSN and can include "Out of Wallet" challenge questions.
- Obtain and verify governmental photo identification and several supporting hard copy documents reflecting name and current address, such as bank statement, credit card bill or utility bill from within the last 90 days, original lease or rental agreement, original property tax bill, first class mail received from federal or state government within the last six months.
- If last name has recently changed obtain and verify marriage certificate, court order of change of last name or divorce decree.
- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement
- No Response

Record and document steps taken and final resolution.

Verification

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.4.7 Notification of Unauthorized Charges or Transactions

Red Flag

City of Franklin is notified of unauthorized charges or transactions in connection with a customer's covered account.

Detection

City of Franklin is notified of unauthorized charges or transactions.

Response

Have the customer sign an Affidavit of Forgery. Work with law enforcement as necessary.

Verification

Ensure employees are trained to

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of id

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor, and department director.

4.5 Notice Given

Red Flags associated with notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by City of Franklin.

Red Flag

Electronic messages are returned to mail servers of the City of Franklin that it did not originally send, indicating that its customers may have been asked to provide information to a fraudulent Website that looks very similar, if not identical, to the Web site of the City of Franklin.

Detection

A department receives an electronic messages that are returned to mail servers of the City, which it did not originally send to the customer.

Response

Call the customer to determine the status and details of the original message they received. If the employee believes that the message was not sent from the City of Franklin, the employee shall immediately notify their supervisor, and call the Franklin Police Department and MIT Department.

- Monitor Accounts
- Change Passwords
- Close Reopen the Account
- Refuse to Open the Account
- Don't Collect on Account
- Notify Law Enforcement

Verification

Conduct and investigation to determine if an external source is using a fraudulent City of Franklin Website.

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee, supervisor, and department director.

4.5.2 Notice that a Fraudulent Account Has Been Opened

Red Flag

City of Franklin is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that City of Franklin has opened a fraudulent account for a person engaged in identity theft.

Detection

City of Franklin is notified a fraudulent account has been opened for a person engaged in identity theft.

Response

City of Franklin will close the account and work with law enforcement. Have the customer sign an Affidavit of Forgery.

Verification

Ensure employees are trained to respond appropriately to a no

Ensure appropriate employees are trained to identify relevant red flags.

Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts. Employees should not confront any individual suspected of committing identity theft. It is our duty to report to the police any suspected patterns of identity theft. It is the duty of the police to conduct the investigations.

See City of Franklin Customer Identification Procedures for verification of customer.

Responsibility

Employee handling the account, supervisor and department director.

5 Appendices

5.1 Report Template

Identity Theft Prevention Program Annual Report to the Board of Directors

January 22, 2010

The intent of this report is to provide the overall status of the Identity Theft Prevention Program, along with providing any updates to any of the program components.

Status

The Identity Theft Prevention Program was last updated on January 11, 2010. The overall status of the Identity Theft Prevention Program is very good.

Effectiveness of Policies and Procedures

City of Franklin has implemented appropriate policies and procedures to comply with 16 CFR Part 681 (Identity Theft Red Flags) to address the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered account.

Service Provider Arrangements

1. New service providers
    a. Risk Manager has drafted a Service Provider Agreement between the City of Franklin and vendors that receive identifying information from the City for official City business and benefit programs.
2. Changes in vendor management processes, procedures, or requirements
    a. The only changes with vendor management process is to have all new and current vendors sign the Service Provider Agreement. A copy of the drafted agreement has been sent to the City Law Department for review. (Please see the attachment of the Service Provider Agreement for further details).

Significant Incidents Involving Identity Theft and Management Response

1. Any significant incidents involving identity theft this year and action taken
    a. There were no reported significant incidents involving identity theft in 2009 for the internally for the City of Franklin.
2. Any service provider significant incidents involving identity theft this year and action taken

a. On October 2, 2009, Blue Cross Blue Shield of Tennessee reported to the City of Franklin a theft of their computer equipment at a network office, located at Eastgate Town Center in Chattanooga, Tennessee. The theft of the equipment included 57 hard drives, containing data which was encoded but not encrypted. (Please, see attached letter from Blue Cross Blue Shields for further details).

Recommendations for Changes in the Identity Theft Prevention Program

1. Additions to the Identity Theft Prevention Program
    a. Continue online training for FACTA.
    b. Adopt the practice of having new and current service providers sign the Service Provider Agreement for the City of Franklin.
2. Deletions from the Identity Theft Prevention Program
    a. None

5.2 Regulations

Federal Trade Commission
16 CFR Part 681
Authority and Issuance
☙ For the reasons discussed in the joint
preamble, the Commission is adding part 681 of title 16 of the Code of Federal Regulations as follows:

PART 681—IDENTITY THEFT RULES

Sec.
681.1 Duties of users of consumer reports regarding address discrepancies.
681.2 Duties regarding the detection, prevention, and mitigation of identity theft.
681.3 Duties of card issuers regarding changes of address.
Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Authority: Pub. L. 108–159, sec. 114 and sec. 315; 15 U.S.C. 1681m(e) and 15 U.S.C.
1681c(h).

§ 681.1 Duties of users regarding address discrepancies.

(a) *Scope.* This section applies to users of consumer reports that are subject to administrative enforcement of
the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1) (users).
(b) *Definition.* For purposes of this section, a *notice of address discrepancy*
means a notice sent to a user by a consumer reporting agency pursuant to
15 U.S.C. 1681c(h)(1), that informs the
user of a substantial difference between
the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.
(c) *Reasonable belief.* (1) *Requirement*
to form a reasonable belief. A user must
develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to
the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.
(2) *Examples of reasonable policies and procedures.* (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:
(A) Obtains and uses to verify the consumer's identity in accordance with
the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR
103.121);
(B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation;
or
(C) Obtains from third-party sources; or
(ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.
(d) *Consumer's address.* (1) *Requirement to furnish consumer's address to a consumer reporting agency.*
A user must develop and implement reasonable policies and procedures for
furnishing an address for the consumer
that the user has reasonably confirmed
is accurate to the consumer reporting agency from whom it received the notice of address discrepancy when the
user:
(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;
(ii) Establishes a continuing relationship with the consumer; and
(iii) Regularly and in the ordinary course of business furnishes information
to the consumer reporting agency from
which the notice of address discrepancy
relating to the consumer was obtained.
(2) *Examples of confirmation methods.* The user may reasonably confirm an address is accurate by:
(i) Verifying the address with the consumer about whom it has requested
the report;
(ii) Reviewing its own records to verify the address of the consumer;
(iii) Verifying the address through third-party sources; or
(iv) Using other reasonable means.
(3) *Timing.* The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer's address that the user has
reasonably confirmed is accurate to the
consumer reporting agency as part of the
information it regularly furnishes for the
reporting period in which it establishes
a relationship with the consumer.

§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope.* This section applies to financial institutions and creditors that
are subject to administrative enforcement of the FCRA by the Federal
Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).
(b) *Definitions.* For purposes of this section, and Appendix A, the following
definitions apply:
(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to
obtain a product or service for personal,
family, household or business purposes.
Account includes:
(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and
(ii) A deposit account.
(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t).

(8) *Identity theft* has the same meaning as in 16 CFR 603.2(a).

(9) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic Identification of Covered Accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(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.

(d) *Establishment of an Identity Theft Prevention Program.* (1) *Program requirement.* Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program.* The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;

(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A of this part and include in its Program those guidelines that are appropriate.

§ 681.3 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 681.2(a) that issues a debit or credit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a credit or debit card.

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account

and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and (ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 681.2 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 681.2 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) 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 financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered

account or not selling a covered account to a debt collector;
(h) Notifying law enforcement; or
(i) Determining that no response is warranted under the particular circumstances.
V. Updating the Program
Financial institutions and creditors should update the Program (including the Red Flags
determined to be relevant) periodically, to reflect changes in risks to customers or to the
safety and soundness of the financial institution or creditor from identity theft, based on factors such as:
(a) The experiences of the financial institution or creditor with identity theft;
(b) Changes in methods of identity theft;
(c) Changes in methods to detect, prevent, and mitigate identity theft;
(d) Changes in the types of accounts that

the policies and procedures
of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered
accounts; service provider arrangements; significant incidents involving identity theft
and management's response; and recommendations for material changes to the
Program.
(c) *Oversight of service provider arrangements.* Whenever a financial
) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a
Suspicious Activity Report in accordance with applicable law and regulation;
(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;
(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2,
for example, to correct or update inaccurate
or incomplete information, and to not report
information that the furnisher has reasonable
cause to believe is inaccurate; and
(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.
Supplement A to Appendix A
In addition to incorporating Red Flags from
the sources recommended in section II.b. of
the Guidelines in Appendix A of this part, each financial institution or creditor may
the financial institution or creditor offers or
maintains; and
(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.
VI. Methods for Administering the Program
(a) *Oversight of Program.* Oversight by the
board of directors, an appropriate committee
of the board, or a designated employee at the
level of senior management should include:
(1) Assigning specific responsibility for the
Program's implementation;
(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor engages a service provider to perform an activity in connection
with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service
provider is conducted in accordance with reasonable policies and procedures designed
to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies
consider incorporating into its Program, whether singly or in combination, Red Flags
from the following illustrative examples in connection with covered accounts:
Alerts, Notifications or Warnings from a Consumer Reporting Agency
1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in
§ 681.1(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant
or customer, such as:
a. A recent and significant increase in the volume of inquiries;
b. An unusual number of recently established credit relationships;
c. A material change in the use of credit, especially with respect to recently established credit relationships; or
d. An account that was closed for cause or identified for abuse of account privileges by
a financial institution or creditor.
institution or creditor with § 681.2 of this part; and
(3) Approving material changes to the Program as necessary to address changing identity theft risks.
(b) *Reports.* (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report
to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management,
at least annually, on compliance by the financial institution or creditor with § 681.2
of this part.
(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of

and procedures to detect relevant Red Flags that may arise in the performance of the
service provider's activities, and either report
the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.
VII. Other Applicable Legal Requirements
Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:
(a

Suspicious Documents
5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer
presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account
or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial
institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of
having been destroyed and reassembled.
Suspicious Personal Identifying Information
10. Personal identifying information provided is inconsistent when compared against external information sources used by
the financial institution or creditor. For example:
a. The

address does not match any address in the consumer report; or
b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
a. The address on an application is fictitious, a mail drop, or a prison; or
b. The phone number is invalid, or is associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. The person opening the covered account or the customer fails to provide all required personal identifying information on
an application or in response to notification
that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer
cannot provide authenticating information beyond that which generally would be provided by the customer. For example, there
is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or
third-party sources used by the financial institution or creditor. For example:
available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change
of address for a covered account, the institution or creditor receives a request for
a new, additional, or replacement card or a cell phone, or for the addition of authorized
users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
b. The customer fails to make the first payment or makes an initial payment but no
subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is,
for example:
a. Nonpayment when there is no history of late or missed payments;
b. A material increase in the use of available credit;
c. A material change in purchasing or spending patterns;
d. A material change in electronic fund transfer patterns in connection with a deposit
account; or
e. A material change in telephone call patterns in connection with a cellular phone
account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage
and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's
covered account.

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 Financial Institution or Creditor

26. The financial institution or creditor 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.
a. The address on an application is the same as the address provided on a fraudulent
application; or
b. The phone number on an application is the same as the number provided on a fraudulent application.

Customer Identification Procedures

All Departments that have covered accounts:

In person:

1. Obtain sufficient Personal Identification Information to allow you to form a reasonable belief that the customer is who they claim to be, including:

- a. Name
- b. DOB
- c. Address
- d. Phone number
- e. SSN
- f. United States Government or State Government issued photo ID, such as a State issued driver's license, military ID, or passport. NOTE: Driver's license or other photo ID's (except for passports) issued by a foreign government are not acceptable.
- g. Copy of a Mortgage or Lease Agreement

2. If you take a SSN, then you must validate that information by contacting the **Veratad ID Plus** Account before you accept it as proof. SSN's are a preferred form of identification but are not required. If the customer prefers not to give their SSN then they must present acceptable photo ID in person.

3. Obtain Personal Identification Information in writing from the customer, input the information and immediately shred the paper, or give it back to the customer. Read it, key it, shred it.

4. If a Red Flag is detected follow the prescribed Next Step in the Red Flag check list. If you are unsure of the Next Step consult with your supervisor before processing the request for a new account. Red Flags must be resolved before a new account can be established. If necessary you should submit the provided information to **Veratad ID Plus** to verify the customer's identity.

5. Avoid taking Personal Identification Information verbally when other customers can overhear the conversation.

6. Insure that no customers can see the Remittance Processing Rep's monitor at any time.

7. Insure that there is no written Personal Identification Information left in view of other customers.

By Telephone, FAX, or Online:

1. Obtain sufficient Personal Identification Information to allow you to form a reasonable belief that the person is who they claim to be, including, but not limited to:

- a. SSN
- b. United States Government or State Government issued photo ID, such as a State issued driver's license, military ID, or passport.
- c. Previous address that matches the verification of the customer's identity from **Veratad**.
-

8. Applications/requests for new accounts not made in person must include a SSN. Before you accept the SSN as proof of identity you must validate that information by submitting to **Veratad**.

9. Check for Red Flags. If a Red Flag is detected follow the prescribed Next Step in the Red Flag check list. If you are unsure of the Next Step consult with your supervisor before processing the request for a new account. Red Flags must be resolved before a new account can be established. If necessary you should submit the provided information to **Veratad** to verify the customer's identity.

10. FAX machines that receive Personal Identification Information from customers must be located in a secure area and the transmissions must be collected several times an hour. The documents must be safeguarded until they can be properly destroyed pursuant to the City of Franklin Records Retention and Disposal Schedule.

Finance Department

Procedure for setting up a new vendor: Once Accounts Payable receives an invoice for payment, the technician will look into Great Plains for their Vendor ID. If no Vendor ID is found then the technician contacts the vendor, and requests their fax number or email address to send 2 forms to be completed. Those 2 forms to be completed are….W9 and Vendor Information Form. Once those 2 forms are returned to Accounts Payable, the technician will turn the information over to Annelle Waddey or Katie Marra to enter the new vendor into Great Plains. This in turn results in the invoice being paid.

Procedure for setting up an employee as a vendor: Once Accounts Payable receives a reimbursement form completed by the employee, the technician will look into Great Plains (Payroll side) for their Employee Number. This number will be used as a Vendor ID. The technician then looks into Great Plains (Accounts Payable side) to see if the employee is set up. If the employee is not set up then, the technician turns over the reimbursement form with the Employee Number on it to Annelle Waddey or Katie Marra to enter the employee into Great Plains (Accounts Payable side). The employee that submits the reimbursement form has to complete the Vendor Information

form only for the purpose of Direct Deposit. All employee reimbursements are directly deposited into the account of the employees' choice. This in turn results in the employee being reimbursed.

Procedure for changing the name of a vendor: If Accounts Payable is notified of a name change on a vendor then a new W9 and Vendor Information form must be submitted. The name change will not occur until this information is received. Once it is received, then the technician will locate the old vendor name and update it with the new vendor name.