2009

**City of Geneva**

Policy Number: 1.0

Effective Date: April 28, 2009

Last Revised Date: April 27, 2009

Responsible Office: Tammy Shuttleworth

Status:
- ☑ Draft
- ☑ Under Review
- ☑ Approved
- ☐ Obsolete

# IDENTITY THEFT PREVENTION POLICY

## VERSION 1.0

This policy has been developed and implemented to comply with the Federal Trade Commission Rules 16 CFR Part 681, better known as the Red Flag Rules that amend the Fair and Accurate Credit Transaction Act of 2003.

# Contents


Purpose and Guiding Principles ..... 4

Scope ..... 6

Statement of Policy ..... 7

Roles and Responsibilities ..... 8

Senior Management ..... 8

Information Security Coordinator ..... 8

Employees ..... 9

Procedures ..... 10

Red Flag Detection and Handling ..... 11

Category 1 – Alerts Notifications or Warnings from a Consumer Reporting Agency ..... 11

Policy Number: 1.0 ..... 11

Category 2 – Suspicious Documents ..... 12

Policy Number: 5.0 ..... 12

Policy Number: 6.0 ..... 13

Policy Number: 7.0 ..... 14

Policy Number: 8.0 ..... 15

Policy Number: 9.0 ..... 16

Category 3 – Suspicious Personal Identifying Information ..... 17

Policy Number: 10.0.a ..... 17

Policy Number: 10.0.b ..... 18

Policy Number: 11.0 ..... 19

Policy Number: 12.0.a ..... 20

Policy Number: 12.0.b ..... 21

Policy Number: 13.0.a ..... 22

Policy Number: 13.0.b ..... 23

Policy Number: 14.0 ..... 24

Policy Number: 15.0 ..... 25

Policy Number: 16.0 ..... 26

Policy Number: 17.0 ..... 27

Policy Number: 18.0 ..... 28
Category 4 - Unusual Use of, or Suspicious Activity Related to, the Covered Account ..... 29
Policy Number: 21.0.d ..... 29
Policy Number: 23.0 ..... 30
Policy Number: 25.0 ..... 31
Category 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 ..... 32
Policy Number: 26.0 ..... 32
Compliance ..... 34
Policy Modifications ..... 34
Communication ..... 34
Acknowledgement of Understanding ..... 35

## Purpose and Guiding Principles

The purpose of this policy is to provide general guidance and specific procedures for protecting the identity and Personal Identifiable Information (PII) of City of Geneva's customers. This data may take many forms, all of which are covered broadly by our Information Security Program. This policy is specifically concerned with transactional relationships, specifically, what we are doing at the time a customer fills out a credit application and we request a consumer report. This policy is intended to ensure that City of Geneva employees, vendors and related third parties take every action available to ensure that neither City of Geneva nor our customers become the victims of identity theft.

The following principles make up the foundation of this Identity Theft Prevention Policy:

- **Formal, Written Statement of Policy** – First and foremost, this policy is intended to formally document City of Geneva's Identity Theft Prevention Program. The management of City of Geneva has taken a risk-based approach to identifying and quantifying our risks associated with identity theft. This policy is intended to communicate the actions required of staff and related third parties to ensure that every effort is made to protect our customers from identity theft.

- **Prevention and Mitigation of the Risks Associated with Identity Theft** – As a result of the risk-based approach City of Geneva has taken to information security planning multiple controls, policies and procedures are in place within the organization to prevent identity theft. From checking each transaction for specific Red Flags, to securing documents, to providing identity theft protection for our customers, specific overlapping controls have been put in place to minimize our risks associated with identity theft.

- **Senior Management Driven** – The Red Flag Rules dictate that either a board of directors or senior management drives the Identity Theft Prevention Program. Regardless of the legal requirement senior management is responsible for the overall Information Security Program at City of Geneva and as such is in committed to leading our effort to protect our customer's personal information.

- **Regular Compliance Reporting** – The Red Flag Rules require that a briefing or report on the state of City of Geneva's compliance be delivered on at least an annual basis.

- **Periodic Updates** – The Identity Theft Prevention Program, as a part of our Information Security Program is updated on at least an annual basis.

- **Incident Response Capability** – City of Geneva recognizes that not every incident can be prevented. As such, we must be prepared to respond to incidents that do occur in a timely,

professional fashion, restoring our customer's identity and confidence to a pre-event status and at the same time minimizing the damage to our brand integrity and reputation.

- **Vendor Integrity** – Our responsibility to our customers does not stop with us. Any vendor, third party provider or supplier to City of Geneva with whom we exchange personal information also has a burden to protect our customer's information. City of Geneva will assess any vendor with whom we conduct business to ensure that they protect our customer's information with the same diligence that we do.

This policy is a part of the larger Information Security Program at City of Geneva, and meets the requirements set forth within the Information Security Policy.

## Scope

This policy applies to all divisions of City of Geneva. Every transaction that we process or attempt to process is covered by this policy. It covers all City of Geneva information technology resources, information that is or may be stored in digital form, as well as information and assets that may exist in physical form. All creation, processing, communication, storage, distribution and disposal of City of Geneva information and assets are covered by this policy. Each employee of City of Geneva, contractor and other related third parties are bound by the guiding principles, statement of policy and related procedures outlined in this policy.

## Statement of Policy

The Identity Theft Prevention Policy exists as a part of our broader Information Security Program and to be in compliance with Federal Trade Commission Rules 16 CFR Part 681, better known as the Red Flag Rules that amend the Fair and Accurate Credit Transaction Act of 2003. This policy exists to give clear and concise directions for preventing and mitigating the risks associated with identity theft within our organization.

The Identity Theft Prevention Policy has been reviewed, approved and is endorsed by City of Geneva senior management.

The Identity Theft Prevention Policy applies to all organization name employees, contractors, third part providers, vendors or suppliers who have access to City of Geneva's customer's Personal Identifiable Information or assist in any way in the application, transmission, approval or granting of a credit decision to one of our customers.

The Identity Theft Prevention Policy is a part of the broader Information Security Policy and must be located with that policy in a central location that is accessible to all City of Geneva employees and related third parties.

The Identity Theft Prevention Policy must be distributed to all new and existing City of Geneva employees who have any role in customer transactions. All City of Geneva employees, contractors and third party providers who do have a role in customer transactions are required to sign an agreement representing the fact that they have reviewed, and agree to adhere to, all policies within the Identity Theft Prevention Policy document.

# Roles and Responsibilities

## Senior Management

Senior management is explicitly responsible for promulgating and enforcing this policy. In addition to its broader responsibilities as a part of the Information Security Program, senior management is responsible for the following:

A. Promulgating and enforcing the policies, standards, procedures, and guidelines for the protection of customer's Personal Identifiable Information.
B. Furnishing necessary funding and other resources or limiting and eliminating services to ensure continued compliance with this policy.
C. Appointing an Information Security Coordinator. Providing appropriate training and resources to the person(s) responsible for information security-related tasks.
D. Sponsoring internal awareness and training programs to familiarize employees, contractors and third-party providers with the security policy, procedures and recommended practices.
E. Defining guidelines and intervals for the review and update of this policy and to reassess existing risks and to identify potential new risks to City of Geneva customer information.

## Information Security Coordinator

Senior management has appointed Tammy Shuttleworth to be the Information Security Coordinator tasked with the day-to-day operation and functioning of the Identity Theft Prevention Program. The Information Security Coordinator will work closely as a liaison between staff and senior management to ensure the continued effectiveness of the Identity Theft Prevention Program.

Outside of broader duties within the Information Security Program, the Information Security Coordinator will be responsible for the following as a part of the Identity Theft Prevention Program:

- Working with City of Geneva sales and F&I personnel to detect and respond to Red Flags that occur as a part of transactional operations
- Verifying that Red Flags have been appropriately cleared before a transaction is allowed to proceed
- Responding to questions about specific Red Flags and seeking guidance as appropriate
- Identifying new Red Flags from experience, media outlets, information security experts and governmental regulations

- Ensuring that senior management is briefed on a regular basis as to the effectiveness of the program
- Providing recommendations to senior management for updating the program

## Employees

Every employee who has a role in processing customer transactions whether it is sales, F&I, back office processing, accounting or otherwise must familiarize themselves with this policy is responsible for complying with each of its provisions.

Each of the covered employees must familiarize themselves fully with the Red Flags that have been identified in this policy and must continually ensure that each Red Flag is verified each time a customer transaction that deals with credit or credit applications occurs.

## Procedures

Within this Section, the phrases "**must**" and "**recommended**" have specific meanings where highlighted in **boldface**. If a department correctly adheres to the guidelines given as "**must**", then it can be considered as meeting the requirements for this policy. If they also adhere to the guidelines given as "**recommended**", then they can be considered to be meeting the minimum requirements to be in accordance with generally accepted information security practices.

# Red Flag Detection and Handling

## Category 1 – Alerts Notifications or Warnings from a Consumer Reporting Agency

### Policy Number: 1.0

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

**Category:** Alerts, Notifications or Warnings from a Consumer Reporting Agency

**Description:** A fraud alert or active duty alert is included with or appended to a consumer report, indicating that the consumer's information has been used or could be used fraudulently. These alerts take three forms:

1. Initial Security Alerts - Placed by either a consumer or in some cases someone acting on their behalf, these alerts are good for 90 days.
2. Extended Fraud Victim Alerts - Added to consumer reports after a valid identity theft report has been filed with law enforcement, these alerts are good for 7 years.
3. Active Duty Alert - Added to consumer reports by those who are active duty in the military while they are deployed, these alerts are good for 1 year.

**Detection:** Every consumer report requested or used in the establishment or maintenance of a consumer account is to be checked for Initial Security Alerts, Extended Fraud Victim Alerts and Active Duty Alerts. Presence of <u>any</u> of these alerts on a consumer report indicates a Red Flag that must be successfully cleared before the transaction can proceed.

**Response:** All fraud alerts must be cleared by further checking the identity of the consumer who is on the premises and letting them know that there is a fraud alert attached to their consumer report. Even after checking the identity in person, the consumer still must be contacted via telephone at the number attached to the fraud alert. In some cases this may be a home or business number which places the transaction on temporary hold. In cases where the consumer has a mobile phone attached to the fraud alert, upon calling the number and witnessing it come through to the consumer in person, the transaction may proceed.

**Verification Procedures:** All fraud alerts must be documented. If a fraud alert is investigated and successfully resolved, it must be documented and approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer reports.

## Category 2 – Suspicious Documents

### Policy Number: 5.0

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

**Category:** Suspicious Documents

**Description:** Whenever documents are provided for identification purposes, careful attention should be given to whether or not the document appears to be original. While good forgeries are hard to detect by simple visual inspection, most forgeries are not of high quality. Any suspicion of forged or altered documents represents a Red Flag which must be documented and investigated before the transaction can proceed.

**Detection:** When looking at identification, close attention should be given to photographs, print and the general appearance of the identification card. Does the ID have visible seams? Is anything crooked? Does type line up correctly? Does its magnetic stripe, holograms or other visible indicators of a genuine ID look authentic? Any inconsistency or question as to the authenticity of a piece of identification represents a Red Flag that must be fully documented before the transaction may proceed.

**Response:** When looking at licenses, passports, Social Security Cards or other forms of identification, any suspicious documents must be documented immediately and investigated. In some cases, further proof of identity may be needed before the transaction is allowed to proceed. NOTE: Some organizations will contact law enforcement when someone tries to use a forged ID.

**Verification Procedures:** Any Red Flags that are indicated by the presence of identification that appears to have been altered or forged must be fully documented and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious documents. The Information Security Coordinator is responsible for approving transactions after the suspicious documents are successfully investigated and resolved.

## Policy Number: 6.0

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

**Category:** Suspicious Documents

**Description:** Photographs and physical descriptions are important identifiers, yet are often overlooked. Many cases of identity theft could have been prevented by simply checking the applicant's identification and verifying that the picture and description presented accurately depict the applicant.

**Detection:** Every applicant must present identification before an account may be opened. Photographs and physical descriptions on the identification must be checked to ensure that the applicant is who he says he is. Any discrepancy in photographs or physical descriptions represents a Red Flag which must be documented and investigated before the transaction can proceed.

**Response:** When presented with a piece of identification that has either a photograph or a physical description that is inconsistent with the appearance of the customer, the discrepancy must be documented and investigated fully. In cases where the applicant cannot reasonably explain the discrepancy, further identification may be needed before the transaction may proceed. NOTE: Some organizations contact law enforcement when presented with forged or false identification.

**Verification Procedures:** Any Red Flags that are indicated by an inconsistency in appearance or physical description must be fully documented and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious photographs or any case where the applicant does not appear to be the same person in the photo identification presented. The Information Security Coordinator is responsible for approving transactions after the suspicious photographs are successfully investigated and resolved.

## Policy Number: 7.0

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

**Category:** Suspicious Documents

**Description:** Other information on driver's licenses or other identification can be indicators of identity theft. Addresses, phone numbers and Social Security Numbers (in the rare cases where they are present) should be checked against both the application and the consumer report.

**Detection:** Every applicant must present identification before an account may be opened. Information on the identification such as addresses or phone numbers must be checked against the application and consumer report to ensure that the applicant is who he says he is. Any discrepancies in information on identification that has been presented represent Red Flags which must be documented and investigated before the transaction can proceed.

**Response:** When presented with a piece of identification that has any information that is inconsistent with the information on the application, the discrepancy must be documented and investigated fully. In cases where the applicant cannot reasonably explain the discrepancy, further identification may be needed before the transaction may proceed. NOTE: Some organizations contact law enforcement when presented with forged or false identification.

**Verification Procedures:** Any Red Flags that are indicated by an inconsistency in information on an applicant's identification must be fully documented and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious documentation including discrepancies on identification. The Information Security Coordinator is responsible for approving transactions after the suspicious documents or identification are successfully investigated and resolved.

## Policy Number: 8.0

**Name:** 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.

**Category:** Suspicious Documents

**Description:** In many cases, the organization already has some information on an applicant, whether it is through a previous history, marketing campaign or other source. In cases where there is a history, information on the application should be checked against this history to ensure that there are no discrepancies.

**Detection:** All applicants are to be screened for prior history with the organization; in cases where this history exists, the application should be compared against it. Special attention should be given to signatures and other examples of customer-specific information. Any discrepancies between this history and the application represent Red Flags which must be fully documented and investigated before the transaction may proceed.

**Response:** When reviewing an application, existing data that the organization has for a customer must be reviewed and compared against the information on the application. Any inconsistencies must be documented and discussed in detail with the applicant. In some cases, further information may need to be gathered before the transaction can proceed.

**Verification Procedures:** Any Red Flags that are indicated by an inconsistency in information on an application when compared against other information the organization has on file must be fully documented and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious documents including suspicious signatures. The Information Security Coordinator is responsible for approving transactions after the suspicious documents are successfully investigated and resolved.

## Policy Number: 9.0

**Name:** An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

**Category:** Suspicious Documents

**Description:** While application forgery seems like it would be easy to spot, depending on where it comes into the system, it can be very difficult to detect. While anyone is likely to catch an application that has been cut and pasted together, it is seldom so simple. Thieves are more likely to forge W2's, tax returns, bank statements or other items that receive less scrutiny. While this can be difficult to detect, in cases where there is doubt, the organization should look for signs of forgery. The devil is in the details, and that's where forgeries fall apart.

**Detection:** Employees must pay attention to details on provided documents, especially those provided in non-original form, for instance those delivered by fax or email. For instance, does FICA withholding actually match the amount the applicant said they made; do both sides of a bank statement balance, etc... ? Any appearance of forgery or document alteration represents a Red Flag which must be documented and investigated before the transaction may proceed.

**Response:** When presented with an application or other piece of supporting material that appears to have been forged or altered, each case must be documented and fully investigated before the transaction can proceed. The applicant may need to provide the original document for inspection, may need to provide more information, or may need to resubmit the application.

**Verification Procedures:** Any Red Flags indicated by the appearance of an application or supporting material must be fully documented, investigated and formally approved before a transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious documents. The Information Security Coordinator is responsible for approving transactions after the altered documents are successfully investigated and, if necessary, resubmitted.

## Category 3 – Suspicious Personal Identifying Information

### Policy Number: 10.0.a

**Name:** The address provided by the consumer during the application process does not match any address in the consumer report.

**Category:** Suspicious Personal Identifying Information

**Description:** The address provided on the application should always match an address in the address history on a consumer report. Personal identifying information (PII) that is inconsistent when compared against external information sources represents a Red Flag.

**Detection:** Each application must be compared against the consumer report to ensure that addresses match. Any address discrepancies must be documented and investigated before the transaction may proceed.

**Response:** When presented with a consumer report that does not match any address provided on the application, each discrepancy must be documented and fully investigated before the transaction is allowed to proceed. More information may need to be gathered from the applicant or from third party sources to prove the validity of the address provided.

**Verification Procedures:** Any Red Flag represented by an address discrepancy between the application and the consumer report must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting address discrepancies. The Information Security Coordinator is responsible for approving transactions after the address discrepancies are successfully investigated and resolved.

**Policy Number: 10.0.b**

**Name:** The Social Security Number provided by the consumer during the application process comes back as having not been issued, or is listed on the Social Security Administration's Death Master File.

**Category:** Suspicious Personal Identifying Information

**Description:** A common indicator of identity theft is when personal identifying information (PII) provided is inconsistent when compared against external information sources used by the financial institution or creditor. One such case is when the Social Security Number is returned as invalid.

**Detection:** When requesting a consumer report, and in using other services that use a Social Security Number as an identifier, invalid Social Security Numbers will often be listed as not having been previously issued, or as being listed in the Death Master File, which tracks the Social Security Numbers and last benefits of people who have died. Any appearance of an invalid Social Security Number represents a Red Flag which must be resolved before the transaction is allowed to proceed.

**Response:** When requesting consumer reports or identity checks, Social Security Numbers may be returned as "Not Issued" or "Deceased". While this may be a simple mistake or transcription error, any discrepancy in Social Security Numbers must be fully documented and investigated. In some cases, it may be necessary to collect other documentation such as a copy of the original Social Security Card, W-2, or tax documents before the Red Flag can be resolved.

**Verification Procedures:** Any Red Flag indicated by a discrepancy in Social Security Numbers must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting invalid Social Security Numbers. The Information Security Coordinator is responsible for approving transactions after the Red Flag is successfully investigated and resolved.

## Policy Number: 11.0

**Name:** Personal identifying information (PII) provided by the customer is not consistent with other PII provided by the customer.

**Category:** Suspicious Personal Identifying Information

**Description:** There are various types of personal information that should coincide. For example, there is correlation between the Social Security Number and date of birth. Likewise, there is a correlation between the Social Security Number and the place of birth. Providing a phone number with an area code that does not match the listed address is another example.

**Detection:** When submitting an application, applicants are required to submit personal information about themselves. This information should be consistent throughout. Things like Social Security Numbers, phone numbers and other information should be checked to ensure it is consistent with other data on the application. Any discrepancy represents a Red Flag that must be documented and resolved before the transaction may be allowed to proceed.

**Response:** Upon finding inconsistent information on an application, the discrepancy should be documented and discussed in full with the applicant. Applications may need to be resubmitted in some cases. In other cases, more information may need to be gathered to verify the applicant's identity. All discrepancies must be fully documented and resolved before the transaction may proceed.

**Verification Procedures:** Any Red Flag indicated by a discrepancy in PII must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting inconsistencies in personal identifying information. The Information Security Coordinator is responsible for approving transactions after the Red Flag is successfully investigated and resolved.

**Policy Number: 12.0.a**

**Name:** The address provided by a consumer on an application is the same as the address provided on a fraudulent application.

**Category:** Suspicious Personal Identifying Information

**Description:** Personal identifying information (PII) provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.

**Detection:** When reviewing applications that have been submitted, information presented on the application should be reviewed against known sources of fraud. This is very similar to the list of bad checks behind the counter at the corner store. If a piece of information, such as an address submitted on an application, matches a known fraudulent piece of information, this represents a Red Flag that must be fully documented and resolved before the transaction may be allowed to proceed.

**Response:** When a Red Flag is indicated by the appearance of an address that is related to known fraudulent activity, the information must be documented and investigated. This could be a legitimate customer whose identity has been misused, or it could be an identity thief. More information may need to be collected about both the person and the fraudulent activity before the Red Flag can be resolved and the transaction approved.

**Verification Procedures:** Any Red Flag indicated by the appearance of an address associated with fraudulent activity must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious or fraudulent addresses. The Information Security Coordinator is responsible for approving any and all transactions after the Red Flags are successfully investigated and resolved.

**Policy Number: 12.0.b**

**Name:** The phone number provided by a consumer on an application is the same as the number provided on a fraudulent application.

**Category:** Suspicious Personal Identifying Information

**Description:** Personal identifying information (PII) provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.

**Detection:** When reviewing applications that have been submitted, information presented on the application should be reviewed against known sources of fraud. If a piece of information, such as a phone number submitted on an application, matches a known fraudulent piece of information, this represents a Red Flag that must be fully documented and resolved before the transaction may be allowed to proceed.

**Response:** When a Red Flag is indicated by the appearance of a phone number that is related to known fraudulent activity, the information must be documented and investigated. This could be a legitimate customer whose identity has been misused, or it could be an identity thief. More information may need to be collected about both the person and the fraudulent activity before the Red Flag can be resolved and the transaction approved.

**Verification Procedures:** Any Red Flag indicated by the appearance of a phone number associated with fraudulent activity must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious information, including suspected or known fraudulent information. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

**Policy Number: 13.0.a**

**Name:** The address provided by a consumer on an application is fictitious, a mail drop, or a prison.

**Category:** Suspicious Personal Identifying Information

**Description:** Personal identifying information (PII) 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.

**Detection:** When reviewing applications that have been submitted, information presented on the application should be reviewed against known sources of fraud. Addresses submitted should be checked to ensure they are legitimate and not associated with mail drops or prisons. If an address submitted on an application matches a known fictitious address or is from a source such as a prison, this represents a Red Flag that must be fully documented and resolved before the transaction may be allowed to proceed.

**Response:** When a Red Flag is indicated by the appearance of an address that appears to be fictitious, a mail drop or a prison, the information must be documented and investigated. This could be a legitimate customer whose identity has been misused, or it could be an identity thief. More information may need to be collected about both the person and the fraudulent activity before the Red Flag can be resolved and the transaction approved.

**Verification Procedures:** Any Red Flag indicated by the use of an address that is known to be fictitious, a mail drop or a prison must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious addresses, including those listed as being mail drops or prisons. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

**Policy Number: 13.0.b**

**Name:** The phone number provided by a consumer during the application process is invalid, or is associated with a pager or answering service.

**Category:** Suspicious Personal Identifying Information

**Description:** Personal identifying information (PII) 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.

**Detection:** When reviewing applications that have been submitted, information presented on the application should be reviewed against known sources of fraud. Phone numbers should be checked to ensure they are legitimate and not associated with pagers or answering services. If a phone number submitted on an application is fictitious or is from a source such as a pager or answering service, this represents a Red Flag that must be fully documented and resolved before the transaction may be allowed to proceed.

**Response:** When a Red Flag is indicated by the appearance of a phone number that appears to be fictitious, or is a pager or answering service, the information must be documented and investigated. This could be a legitimate customer whose identity has been misused, or it could be an identity thief. More information may need to be collected about both the person and the fraudulent information before the Red Flag can be resolved and the transaction approved.

**Verification Procedures:** Any Red Flag indicated by the use of a phone number that is associated with a pager or answering service, or is invalid must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious information, including invalid phone numbers. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

## Policy Number: 14.0

**Name:** The Social Security Number provided by a consumer during the application process is the same as that submitted by other persons opening an account or other customers.

**Category:** Suspicious Personal Identifying Information

**Description:** Social Security Numbers are unique identifiers, of which no two people will have the same number. Applications containing Social Security Numbers should be checked to ensure that no other customer of the organization has opened or tried to open an account using the same number.

**Detection:** When reviewing applications that have been submitted, if a Social Security Number is required, it should be compared against other accounts that the organization maintains. Any appearance of a Social Security Number that has been used or has been attempted to be used represents a Red Flag that must be documented and resolved before the transaction may be allowed to proceed.

**Response:** Whenever a Social Security Number is used that has been used in opening or trying to open another account, the event must be documented. This may represent a mistake or transcription error, or it may represent an attempt to commit identity theft. Further information including original Social Security Cards, W-2s or tax returns may be needed to verify the applicant's identity. As a follow up in the event that the application is genuine, the account that caused the Red Flag to occur will need to be investigated.

**Verification Procedures:** Any Red Flag indicated by the use of a Social Security Number that is the same as the SSN submitted by someone else must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious information, including duplicate Social Security Numbers. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

## Policy Number: 15.0

**Name:** The address or telephone number provided by a consumer during the application process is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

**Category:** Suspicious Personal Identifying Information

**Description:** Addresses and telephone numbers are unique identifiers. It is rare for people who are not family members to share the same information. Applications containing addresses and telephone numbers should be checked to ensure that no other customer of the organization has opened or tried to open an account using the same telephone number or address.

**Detection:** When reviewing submitted applications, if an address or telephone number is required, it should be compared against other accounts that the organization maintains. Any appearance of an address or telephone number that has been used or has been attempted to be used represents a Red Flag that must be documented and resolved before the transaction may be allowed to proceed.

**Response:** Any Red Flag indicated by the use of an address or telephone number that is the same as the address or telephone number submitted by someone else must be fully documented, investigated and formally approved before the transaction may proceed.

**Verification Procedures:** Any Red Flag indicated by the use of an address or telephone number that is the same as the address or telephone number of another customer must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious information, including information that appears to have been used by multiple applicants. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

## Policy Number: 16.0

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

**Category:** Suspicious Personal Identifying Information

**Description:** The entirety of personal information submitted on an application is important. While providing this information is fairly tedious, but trivial for a normal consumer, it can prove difficult for an identity thief. Thus, failure to provide required information is a good indicator of identity theft.

**Detection:** When reviewing applications that have been submitted, look to ensure that everything has been filled out. While this may have been an oversight on the part of the applicant, it represents a Red Flag that must be resolved before the transaction may be allowed to proceed.

**Response:** Upon detecting a Red Flag indicated by the failure to provide required personal information, the item or items should be brought to the applicant's attention. This may have been a simple oversight that is easily corrected. If there is any unwillingness or the customer does not know the required information, the event will need to be documented and more information may need to be gathered to ensure the applicant's identity before the transaction may be allowed to proceed.

**Verification Procedures:** Any Red Flag indicated by the applicant's failure to provide all of the required personal identifying information on an application must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious applications, especially those that appear to be incomplete. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

## Policy Number: 17.0

**Name:** Personal identifying information provided by the consumer during the application process is not consistent with personal identifying information that is on file with the financial institution or creditor.

**Category:** Suspicious Personal Identifying Information

**Description:** In many cases, the organization may already have some information on file about an applicant. They may already have another account with the organization, or they may be responding to a marketing campaign in which the organization already knows something about them. Any information that the applicant provides should be compared against information the organization already knows to ensure that the applicant is who they say they are.

**Detection:** An applicant is required to submit certain personal identifying information (PII) as part of the application process. In cases where the applicant already has an account with the organization, the information provided should be checked against the information on file. Likewise, whenever marketing campaigns are conducted or the organization acquires data about consumers from another source, the information provided by the applicant should be compared to the information that is already known to ensure the applicant is who they say they are. Any discrepancy represents a Red Flag that must be resolved before the transaction can be allowed to proceed.

**Response:** Whenever there is a Red Flag indicated by a discrepancy in an applicant's information when compared to information that the organization has on file, it must be documented and investigated. After discussing the discrepancy with the consumer, further information may need to be gathered to ensure the applicant's identity before the transaction can be referred to the Information Security Coordinator for approval.

**Verification Procedures:** Any Red Flag indicated by a discrepancy in the personal identifying information provided during the application process must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious information, including any information that is inconsistent with that which is already on record. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

## Policy Number: 18.0

**Name:** The person or customer opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

**Category:** Suspicious Personal Identifying Information

**Description:** Organizations often have access to data about their customers that is not publically available. The organization may have access to information about account histories, prior purchases or other types of information such as job histories or educational histories that wouldn't typically be known to anyone except the customer.

**Detection:** When reviewing applications, particular attention should be given to information that isn't generally available in a wallet or on a consumer report. It may be useful to casually question the applicant about a few of the items. This is a trivial exercise for a genuine applicant, but for an identity thief who often makes up data on the spot, it is a sure giveaway. Any discrepancy or inconsistency in information provided on an application represents a Red Flag that must be documented and resolved before the transaction may proceed.

**Response:** Upon detecting a discrepancy in personal identifying information, especially when it concerns data that isn't publicly available, careful attention should be given to following up with the applicant about the information. The Red Flag must be documented, and in some cases further information may need to be provided in order to verify the applicant's identity before the transaction can be forwarded to the Information Security Coordinator for approval.

**Verification Procedures:** Any Red Flag indicated by the applicant's failure to provide authenticating information must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Individual personnel who handle, view or process consumer applications are responsible for detecting, responding to and documenting suspicious applications, especially those in which the applicant cannot provide basic corroborating information about themselves. The Information Security Coordinator is responsible for approving transactions after any and all Red Flags are successfully investigated and resolved.

## Category 4 - Unusual Use of, or Suspicious Activity Related to, the Covered Account

### Policy Number: 21.0.d

**Name:** An existing account has a material change in electronic fund transfer patterns in connection with a deposit account.

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

**Description:** A common indicator of identity theft on covered accounts is when credit is used in a manner inconsistent with established patterns of activity on the account. One such indicator is when there is a material change in electronic fund transfer patterns in connection with a deposit account.

**Detection:** Existing accounts must be monitored for misuse. Whenever there is a material change in electronic fund transfer patterns, this represents a Red Flag which must be documented and requires the customer be contacted to ensure that he is in control of his account before further transactions may be processed.

**Response:** When Red Flags are detected that are related to a material change in electronic fund transfer patterns, the customer must be contacted to ensure that he is still in control of his account. In many cases, the customer may be able to explain the transfers and the reasons behind them, and no further action beyond documenting the Red Flag may be necessary. In some cases, the customer may need to present further proof to verify his identity. In cases where identity theft is suspected, an account hold should be placed on the account, and further steps taken to verify the customer's identity before the account hold can be forwarded to the Information Security Coordinator to be lifted. In cases where identity theft is detected, steps will need to be taken to notify the victim and provide appropriate remedy.

**Verification Procedures:** Any Red Flag indicated by a material change in electronic funds transfer patterns must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Internal audit is responsible for developing procedures to identify, document, and suspend any account for which any suspicious activity appears, including a material change in electronic fund transfer patterns in connection with a deposit account. The Information Security Coordinator is responsible for approving and lifting holds on accounts once any and all Red Flags are successfully investigated and resolved.

**Policy Number: 23.0**

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

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

**Description:** An address change is often an identity thief's first step. By lengthening the period of time that it takes for either the victim or a merchant to become aware of the theft, the thief has more time to misuse the identity. Mail that is repeatedly returned as undeliverable despite the fact that transactions continue to be processed is often an indicator of identity theft.

**Detection:** When more than one piece of mail is returned as undeliverable, especially when the mail is an account statement or other important notification, and yet transactions continue to be processed, this represents a Red Flag that must be documented and resolved before further transactions can be processed.

**Response:** When a Red Flag is detected due to mail being repeatedly returned as undeliverable, the customer should be contacted by phone or other method immediately. In some cases, it may be possible to mark the person's account with a comment that will be seen the next time he comes into an office for service. The customer should be required to provide an updated address, and once the customer's identity is verified, this may be the only action required beyond documenting the Red Flag. In some cases it may be necessary to gather further information in order to verify the customer's identity. Only after this is done and a correct address collected may the account be forwarded to the Information Security Coordinator to have any account holds lifted. In cases where an act of identity theft is confirmed, steps will need to be taken to notify the victim and provide appropriate remedy.

**Verification Procedures:** Any Red Flag indicated by sent mail being repeatedly returned must be fully documented, investigated and formally approved before the transaction may proceed.

**Responsibility:** Internal audit is responsible for developing procedures to identify, document and suspend any account for which any suspicious activity appears on an account, including those for which transactions are attempted despite the fact that mail has been returned. The Information Security Coordinator is responsible for approving and lifting holds on accounts once any and all Red Flags are successfully investigated and resolved.

**Policy Number: 25.0**

**Name:** The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

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

**Description:** One of the first signs of identity theft is when a customer notices unauthorized charges on his account and notifies the institution. While these are not always related to identity theft, more often than not, foul play is to blame.

**Detection:** Whenever the organization is notified of the presence of unauthorized charges on an account, this represents a Red Flag that must be documented and resolved. This notification typically comes from customers, but may come from other merchants, law enforcement or other organizations.

**Response:** Whenever the institution is notified of unauthorized charges or activity on an account, immediate action should be taken to stem further losses. An investigation will need to be initiated into the activity, and will serve as documentation for the Red Flag. In some cases, the customer may find out that the unauthorized use is not necessarily identity theft, but is activity of which they were unaware. This will need to be documented, and in those cases, no further action may be needed. In cases where identity theft is suspected, new cards and possibly new accounts will need to be created for the customer and appropriate remedies provided. In some cases, the matter may be handed over to law enforcement for further action.

**Verification Procedures:** Any Red Flag indicated by the notification of unauthorized use or transaction on an account must be fully documented, investigated and formally approved before the account may be used again. In most cases, new accounts will need to be opened for the customer.

**Responsibility:** Customer service representatives who speak with customers are responsible for documenting any cases in which customers inform the organization that fraudulent transactions may be on a given account. The Information Security Coordinator is responsible for approving and lifting any account holds upon the investigation and successful resolution of any and all Red Flags.

## Category 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

**Policy Number: 26.0**

**Name:** 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.

**Category:** 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

**Description:** Identity theft events do occur. Occasionally, someone will get past all of the organization's defenses and actually manage to open a fraudulent account. In some cases, thieves may use the account in ways that do not immediately indicate identity theft. However, thieves are often found, and their activities unraveled. It is at these times where the organization may be notified that they have been an unwitting participant in an identity theft scheme. Having a predetermined incident response plan that can be executed quickly will ensure that the event's impact on the organization's finances, brand integrity and reputation will be minimized.

**Detection:** The organization must have procedures in place to take action when notified that they have opened a fraudulent account. These events do happen to even the most prepared organizations. Regardless, the notification that the organization has opened a fraudulent account represents a Red Flag that must be formally documented and investigated.

**Response:** In most cases the account should be immediately suspended. In some cases, law enforcement may request that the account is kept open in order to help identify the thieves or build a case against them. Thorough documentation should be prepared in the case for two reasons: first, to be used to prove losses, and second, to be used to strengthen organizational policies and procedures in the future. In the event that an account has been opened using the identity of a real person, steps will need to be taken to notify the person and to provide appropriate remedy.

**Verification Procedures:** Any Red Flag indicated by the institution being notified of a fraudulent account must be fully documented, investigated and action formally taken. This may result in accounts being closed, new accounts opened for existing customers and notification and/or victim recovery services being provided to the affected individual(s).

**Responsibility:** The Information Security Coordinator is responsible for documenting and investigating any Red Flags indicated by law enforcement, customers or a victim of identity theft informing the organization of the possible presence of fraudulent transactions on a covered account. All employees are responsible for contacting the Information Security Coordinator if they are contacted by anyone who reports a possible occurrence of identity theft.

## Compliance

Any person who uses City of Geneva's information or assets consents to all provisions of this policy and agrees to comply with all of its terms and conditions, as well as with relevant state and federal laws and regulations. Users have a responsibility to use these resources in an effective, ethical and lawful manner. Any violation of this policy may result in disciplinary or administrative sanctions including loss of privileges, monitoring of use and up to and including termination depending on the severity and intent of offense. Additionally, non-compliance with this policy resulting in loss or disclosure of data may result in personal civil and/or criminal liability.

## Policy Modifications

This policy may be changed by City of Geneva Senior Management at any time, but typically will be modified in response to newly identified threats or risks. Changes to this policy will be communicated and distributed to all affected parties. Most major changes to the policy will be made during official policy review sessions on an annual basis, but if required a policy review session may be convened on a special basis.

## Communication

Upon approval, this policy is to be distributed to all City of Geneva employees, contractors, vendors and related third parties. Upon subsequent revisions, updates or amendments to this policy affected individuals will be notified of the change along with an office or individual to whom they can direct additional questions.

## Acknowledgement of Understanding

I have been provided with a copy of the City of Geneva Identity Theft Prevention Policy and have read and reviewed the policy. I have been provided the opportunity to ask questions about the policy and am aware of resources to which I may look for more information. I understand that it is my responsibility to comply with the provisions of the policy and that failure to do so is subject to disciplinary action up to and including immediate termination. My signature below indicated that I have been provided with and have read the City of Geneva Identity Theft Prevention Policy and furthermore indicates my understanding and willingness to comply with the provisions of the policy.

_____

Employee

_____

Date