# 2900. IDENTITY THEFT POLICY

## TABLE OF CONTENTS

# IDENTITY THEFT PREVENTION PROGRAM

## PROGRAM ADMINISTRATION

Oversight of the *Identity Theft Prevention Program* shall be carried out by the Compliance Officer as delegated by the President/CEO and Board of Directors. Oversight includes:

- Assignment of specific responsibilities for implementation.
- Review of staff reports regarding compliance with applicable regulations.
- Approval of *Program* modifications to address changes and developments in identity theft risks.
- Vendor/service provider arrangements as follows:
  - Only those performing activities in connection with one or more covered accounts.
  - Taking steps to ensure activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate identity theft.

The Compliance Officer (or designee) is responsible for reviewing red flags[1] and responsive actions periodically and updating as necessary to reflect changes in the risks to members or to the safety and soundness of the Credit Union.

The Compliance Officer (or designee) will review reports assembled by management or delegated staff with regard to the development, implementation, and administration of the *Identity Theft Prevention Program* and shall be presented on an annual basis to the Board of Directors and the President/CEO as outlined in the *Reporting* section of this document under the *Identity Theft* subsection.

## IDENTIFYING NEW COVERED ACCOUNTS AND RELEVANT RED FLAGS

Periodically, but at least annually, the Credit Union will determine what accounts offered or maintained are considered "covered" accounts.[2] For all accounts that impose above average risks to the member or Credit Union safety and soundness, Resource One management will direct the performance of a risk assessment that takes into consideration:

1 A red flag is a pattern, practice, or specific activity that indicates the possible risk of identity theft.

2 A covered account is an account that is offered or maintained by the Credit Union primarily for personal, family, or household purposes that is designed to permit multiple payments or transactions or any other account for which there is a reasonably foreseeable risk to members or to the safety and soundness of the Credit Union from identity theft. Examples include, but are not limited to, credit card accounts, mortgage loans, automobile loans, share, or deposit accounts.

- The methods used to open the accounts.
- The methods used to provide access to the accounts.
- Previous experiences with identity theft.

Documentation on the rationale used for determining that a particular type (category) of account offered or maintained will not be considered a covered account should be maintained by the Compliance Officer (or designee).

If any new categories of covered accounts are identified, the Credit Union will conduct a risk assessment to identify relevant red flags associated with these new covered accounts. These identified red flags will be used to detect, prevent, and mitigate identity theft in connection with the opening of a "covered" account or any existing "covered" account.

**REVIEWING RELEVANT RED FLAGS**

Red flags and responsive actions will be reviewed periodically and updated as necessary to reflect changes in the risks to members or to the safety and soundness of the Credit Union.

The Credit Union will base any additions, removals, or updates on factors such as:

- The Credit Union's experiences with identity theft.
- Changes in the methods of identity theft.
- Changes in the methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts the Credit Union offers or maintains.
  - Passwords/security codes/other devices permitting access to covered account
- Changes in the business arrangements of the Credit Union.

A record of these reviews and a summary of any changes required will be documented and maintained by the Compliance Officer (or designee).

### CURRENT RED FLAGS

The Credit Union shall isolate and deter instances of potential identity theft evidenced by red flags. The current red flags identified by the Credit Union include:

### Receipt of Alerts or Notifications

- Fraud or active duty alert on the credit report.
- Credit bureau notice of a credit freeze in response to a request for a credit report.
- Notice of address discrepancy supplied by a third party such as a credit bureau.
- Notice from members, victims of identity theft, law enforcement, or other people regarding possible identity theft in connection with covered accounts is received by the Credit Union.
- The Credit Union is notified of unauthorized changes in connection with a member's account.
- The Credit Union is notified of unauthorized charges or transactions in connection with a member's account.
- The Credit Union is notified that is has opened a fraudulent account for a person engaged in identity theft.
- The Credit Union is notified that the member is not receiving account statements.
- The Credit Union is notified that its member has provided information to someone fraudulently claiming to represent the Credit Union or to a fraudulent website.
- Electronic messages are returned to the Credit Union that were not originally sent by the Credit Union indicating that members may have been asked to provide

information to a fraudulent website that looks very similar, if not identical, to the Credit Union's website.

**When Opening New Accounts**

- Presenting suspicious documents.
- Presenting altered identification documents.
- Presenting suspicious personal identifying information.
- Photograph/description of member inconsistent with person presenting the identification.
- Other information on the identification is not consistent with the information provided by the person opening a new account.

- Social security number appears to be inaccurate.
  - ✓ Number given has not been issued.
- ✓ Number given is listed on the Social Security Administration's Death Master File.
- ✓ No correlation between the social security number range and the date of birth.
- Personal information provided is associated with known fraud activity.
  - ✓ Address and/or telephone number on an application is the same as provided on a fraudulent application.
  - ✓ Address on the application is fictitious, a mail drop, or a prison.
  - ✓ Telephone number on the application is invalid or is associated with a pager or answering service.
- Invalid addresses or phone numbers.
- Address, phone number, or social security number submitted by other members or applicants
- The person opening an account fails to provide all required information on the application.
- The person opening an account cannot provide authenticating information beyond that which would generally be available from a lost or stolen wallet or a consumer report.

**When Servicing Existing Accounts**

- Presenting suspicious personal identifying information.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or member presenting the identification.
- Other information on the identification is not consistent with the information provided by the member presenting identification.
- Identity information provided that does not match information currently on file.
- Personal information that is inconsistent with information provided by outside sources.
- Social security number appears to be inaccurate.
  - ✓ Number given has not been issued.
- ✓ Number given is listed on the Social Security Administration's Death Master File.
- ✓ No correlation between the social security number range and the date of birth.
- Personal information provided is associated with known fraud activity.
- ✓ Address and/or telephone number on an application is the same as provided on a fraudulent application.
- ✓ Address on the application is fictitious, a mail drop, or a prison.

- ✓ Telephone number on the application is invalid or is associated with a pager or answering service.
  - The address, social security number, or home/cell phone number provided is the same as that of another person.
- Returned mail on active accounts.
- Notification that the member has not been receiving paper statements
- Activity on dormant or inactive accounts.
- Account activity inconsistent with the typical pattern of a member such as:
  - Non-payment when there is no history of late or missed payments.
  - A material increase in the use of available credit.
  - A material change in purchasing or spending patterns.
  - A material change in electronic fund transfer patterns in connection with a deposit account.
  - There are unusually frequent and large check orders placed.
- Suspicious address change.
  - Address on the form is fictitious, a mail drop, or a prison.
  - Address on the form is the same as that of another person.
- Member is unable to lift a credit freeze placed on his/her consumer report.
- The Credit Union detects attempts to access a member's account by unauthorized persons.

**Change of Address**

- Within thirty (30) days after change of address notification, request is received for an additional or replacement debit or credit card.
- Request to add additional account/credit card users shortly after address change submitted.

**Consumer Report**

A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member, 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 is closed for cause or identified for abuse of account privileges by a financial institution or creditor.

**Other Red Flags**

- There are unusually frequent and large check orders in connection with a member's account.
- There are unusually frequent and large wire or Internet Banking transfers in connection with a member's account.
- The person or member opening an account is unable to lift a credit freeze placed on his or her consumer report.

**Employee Activities**

- The name of a Credit Union employee has been added as an authorized user on an account.
- An employee has accessed or downloaded an unusually large number of member account records.
- The Credit Union detects or is informed of unauthorized access to a member's personal account.

## DETECTING RED FLAGS

**Opening a New Account**

When opening a new account, Credit Union staff will obtain and verify the identity of any person opening a covered account through Customer Identification Procedures (MIP) subject to USA PATRIOT Act. Staff will check to ensure information provided on the membership application is not associated with fraudulent activity. For example, if you pull a credit bureau report to process the new account application and the report has a fraud alert, the Credit Union must contact the individual before membership is approved. In addition, fraud alerts should be shared across the Credit Union's various lines of business.

Credit Union employees will analyze whether there is logical consistency between the identifying information provided such as the consumer's name, street address, ZIP code, telephone number, date of birth, and social security number.

All applicants will be verified through OFAC before opening. There are no exceptions. Prior to the account being opened, the Credit Union will crosscheck the name(s) of any new member against any list of known or suspected terrorists or terrorist organizations

issued by any federal government agency and designated as a MIP Section 326 List by the Treasury Department or other agencies.

Based on the Credit Union's risk assessment of a new account opened by a customer that is not an individual, the Credit Union will obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity.

## Member Identification Policy (MIP)

As part of Resource One Credit Union's overall plan of compliance with the Bank Secrecy Act, it is our policy to have a clear and concise understanding of all Credit Union customer identification practices in order to avoid liability to this organization by any customer who would use Credit Union resources for illegal purposes or to compromise national security. The objective of this policy is to ensure the identification of members/customers, referred to hereafter as "customers," and immediate detection of any suspicious activity at the institution.

Resource One Credit Union recognizes that appearances can be deceiving and potential customers could be establishing a business relationship to conduct illicit activities. Accordingly, pursuant to the USA PATRIOT Act, Resource One Credit Union will incorporate the following into its business practices:

- Internal policies, procedures, and controls.
- Ongoing employee training.
- Independent audit function.

Before opening an account, a new customer will be advised of the Credit Union's MIP program as explained in the implementing procedures.

## Member Identification – New Accounts

Resource One Credit Union will not establish a business relationship until the identity of the potential member/customer is satisfactorily established. It is understood that a community-based Credit Union such as Resource One has a strong knowledge of the community and the customers it serves; therefore, limited exceptions may be made only when authorized and signed by a member of management.

Credit Union staff will use both documentary and non-documentary methods to verify the identity of all new account owners. If an account is requested through the mail, the account will not be opened until document information and a signed card are received.

Resource One Credit Union believes it has reasonable basis to assume that members accepted on or before October 1, 2003 are reasonably verified and established with the Credit Union. Should events occur giving rise to question true identity of a

member/customer, the Credit Union will begin procedures to verify that person's identity per these guidelines. In all other instances, the following guidelines will be observed:

At a minimum, the following information will be collected prior to opening or adding a signatory to any type of account:

- Name.
- Date of birth (for individuals).
- Residence and if different, street address (for individuals).[3]
- Principal place of business and, if different, mailing address (for persons other than individuals, such as corporations, partnerships, and trusts).
- For U.S. persons, a U.S. taxpayer identification number (e.g., social security number, individual taxpayer identification number, or employer identification number).
- For non-U.S. persons, one or more of the following:
  - U.S. taxpayer identification number.
  - Passport number and country of issuance.
  - Alien identification card number.
  - Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

**Verifying Identity**

Identification presented to Resource One Credit Union will be verified in the following ways:

- Personal Accounts:

Identification card - Unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard. The following will be taken into consideration:

3 For members who have been issued a post office box address as part of their participation in a state-created address confidentiality program (ACP) for victims of domestic abuse, the Credit Union shall treat that person as not having a residential or business street address and the state entity serving as a designated agent of the participant will act as "another contact individual" for the purpose of complying with the FinCEN's rules regarding member identification street address requirements. The Credit Union should obtain the street address of the sponsoring ACP agency for the purposes of meeting this requirement. **Note:** If the Credit Union accepts and uses the ACP post office box address to fulfill the member identification street address requirement, the Credit Union will not be in compliance.

- The customer's residence or place of business. If it is not in the area served by the Resource One Credit Union or branch, ask why the customer is opening an account at that location.
- The source of funds used to open the account.
- Service bureau reports.
- Follow-up with calls to the customer's residence or place of employment thanking the customer for opening account.

A customer may be a referral from a Resource One Credit Union employee or one of the Credit Union's accepted customers. In this instance, a referral alone is not itself sufficient to identify the customer.

- Business Accounts:
  - For corporations, partnerships, trusts, and persons other than individuals obtain the following:
    - Tax ID number (or a copy of the application for one – if the tax ID number is not received within five (5) weeks, the account will be closed).
    - Documents showing the existence of the entity, such as registered articles of incorporation.
    - A government-issued business license, partnership agreement, or trust instrument.
  - Check the name of a commercial enterprise with a reporting agency and check prior Resource One Credit Union references.
  - Follow-up calls to the customer's business thanking the customer for opening the account.
  - When circumstances allow, perform a visual check of the business to verify the actual existence of the business.
  - Consider the source of funds used to open the account.

**Non-Documentary Verification**

Non-documentary verification may be used under the following circumstances:

- An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard.
- Resource One Credit Union is not familiar with the documents presented.
- The account is opened without obtaining documents.

- The account is not opened in a face-to-face transaction.
- The type of account increases risk that the Credit Union will not be able to verify true identity through documents.

Non-documentary verification methods may include, but are not limited to:

- Contacting the customer.
- Obtain a paystub, W2, or first page of previous tax return.
- View social security card.
- Obtain paystub, utility bill, bank statement, and/or insurance card with current address.
- If person is new to country, ask for immigration papers (green card or legal alien card).
- Independently verifying documentary information through:
  - Credit bureaus.
  - Public databases or other sources.
  - Checking references with other financial institutions.
  - Obtaining a financial statement.

## Identity Verification of Minors

The definitions of the Bank Secrecy Act state that a member is a person that opens a new account; this definition includes an individual who opens a new account for an individual who lacks legal capacity such as a minor. Therefore, under the Act, for verification purposes only, the adult individual that is opening the new account on behalf of the minor is considered the member, not the minor for whom the account is opened. While the minor may be named on the account as the member of record and there may or may not be a joint owner, the parent will generally be required to have his/her identity verified.

A minor child is allowed to open the account on his own behalf. However, if the child cannot provide government issued identification at account opening, an adult must be a participant in the account opening to comply with MIP and OFAC requirements. This applies whether or not that adult will be an owner of the account.

## Member Identity Verification Existing Accounts

The purpose of this procedure is to determine the true identity of the member transacting business or requesting information about an account. Certain requirements

apply depending on whether the member is transacting business through face-to-face communication, telephone, or email.

- Walk-in Requests

When the nature of a transaction warrants it, the identity of walk-in members will be verified unless the Credit Union employee personally knows the member. This includes members requesting information from their account. If the member is not personally known to the employee, the member must provide their name, member number, and a valid driver's license, state issued ID card, or permanent resident card.

If a member's situation warrants collecting additional information or they do not have identification, verification should be completed by requesting at least **one** additional item from the list below:

- The most recent deposit (this amount can be rounded up or down to the nearest dollar).
- Company or government agency of their direct deposit if applicable.
- A recent ATM transaction amount or location.
- A recent debit card transaction.
- How the member joined the Credit Union.

- Teller Transactions

Members requesting funds from their account must provide their name, member number, and a valid driver's license, state issued ID card, or permanent resident card. If a member's situation warrants collecting additional information, verification should be completed by requesting at least **one** additional item from the list below:

- The most recent deposit (this amount can be rounded up or down to the nearest dollar).
- Company or government agency of their direct deposit if applicable.
- A recent ATM transaction amount or location.
- A recent debit card transaction.
- How the member joined the Credit Union.

- Telephone Communication

Employees of the Credit Union are required to verify the member's name, account number, and at least **one** additional piece of information from a member calling to obtain

account information. Members correctly answering questions from the following list will be granted access to information about the account.

- The most recent deposit (this amount can be rounded up or down to the nearest dollar).
- Company or government agency of their direct deposit if applicable.
- A recent ATM transaction or location.
- A recent debit card transaction.
- How the member joined the Credit Union.

- Email

Members requesting information about their account via email (other than through our website) should be called at the number of record in response to their request. Speak to the member directly; do not leave the information on an answering machine or with anyone else. In addition, assuming the member included their account number in the email, the telephone call could be used as an opportunity to inform the member that Internet email is generally not secure. In order to guard against unauthorized individuals obtaining their confidential information, only secure connections should be used.

- E-Commerce Authentication of Members

The Credit Union will utilize multifactor authentication when authenticating members using Internet Banking. Single-factor will be utilized when authenticating members using Telephone Banking.

- Passwords

It is not our general business practice to establish passwords on accounts in addition to our normal operating procedures for proper identification; however, if a member has a password on their account, the procedure for member verification must be followed in addition to receiving the member's password.

No Personal Identification Number (PIN) or password used for online or telephone authentication will be reset or reissued prior to verifying the identity of the individual making the request. The identity of a member will be verified by asking a series of security questions that involve account activity and out of wallet questions such as those listed below:

- The most recent deposit (this amount can be rounded up or down to the nearest dollar).
- Company or government agency of their direct deposit if applicable.

- A recent ATM transaction amount or location.
- A recent debit card transaction.
- How the member joined the Credit Union.

**Credit Bureau Reports**

As a user of credit reports, Resource One will:

- Compare information received in the report with member information:
  - Obtained and used for verification of member identity pursuant to MIP.
  - Maintained in its records, to include:
    - ✓ Applications.
    - ✓ Address change notifications.
    - ✓ Other member account records.
    - ✓ Retained MIP documentation.
  - Obtained from third-party sources.
- Verify credit report information as provided.

The Credit Union shall use reasonable procedures for furnishing information to the credit bureau from which a notice of an address discrepancy was received, at such time the Credit Union:

- Can form reasonable belief that the report is that of the member about whom it was requested.
- Establishes a continuing relationship with the member.
- Regularly, in the normal course of business, furnish information to the credit bureau from which the notice of address discrepancy was obtained.

Reasonable address confirmation can be determined through:

- The member.
- Credit Union records.
- Third party sources.
- Other means deemed reasonable by management.

Resource One Credit Union shall provide a member's confirmed address to a credit bureau as part of regularly furnished information for the reporting period in which Resource One establishes a relationship with the member.

## Monitoring Transactions

An integral part of Resource One Credit Union's *Identity Theft Prevention Program* is a good knowledge of the transactions carried out by its members. Internal systems have been developed to assist in determining inconsistent activity on behalf of the customer.

## Verify Address Change Requests

Change requests will be accepted via mail and fax and must contain the account number to be changed, a copy of the member's driver's license, and the signature of the tax ID owner of the account. Change requests may be submitted in person as well as via the Internet Banking platform after authentication. Any exceptions must be approved by a Credit Union manager and be noted on the change request. The Credit Union employee performing the change must initial and date the request to indicate it has been completed.

### RESPONDING TO RED FLAGS

Upon becoming aware of any activities (as previously described) compromising the identity of a current or potential member, Credit Union staff will make use of any/all available actions including:

- Monitoring an account (for fraudulent activity).
- Direct member contact.
- Changing a password or security code.
- Not opening a new account.
- Closing an existing covered account.
- Reopening an account with a new number.
- Notifying law enforcement.
- Filing a Suspicious Activity Report (SAR).
- Determining circumstances warrant no response.

## Discrepancies in Customer Identification

When any of the current red flags are identified during the identity verification process, public law requires that those discrepancies be resolved as part of MIP. Attempt to reconcile all discrepancies in identification information prior to opening an account or extending credit. If discrepancies cannot be reconciled, the account will not be opened or credit extended. Concerns should be discussed with supervisory/management personnel.

The Credit Union must maintain a description of the how those discrepancies were resolved for a period of five (5) years.

## Unable to Verify Identity

Under circumstances in which the Credit Union cannot form a reasonable belief that the true identity of a customer is known, that account will not be opened.

An account will be closed if attempts to verify the customer's identity fail.

## Applicants Name Appears on a Government List

If the crosscheck of an applicant's name against any list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by the Treasury Department in consultation with the federal functional regulators produces a match, the Credit Union will follow all federal directives issued in connection with such lists. Any applicant whose name appears on any of the above-mentioned lists may not be permitted to open an account at Resource One Credit Union.

## Discrepancies

When the Credit Union receives a notice of address discrepancy from a consumer reporting agency, Resource One will reconcile any and all address discrepancies with regard to member account files as well as information received through credit reporting agencies. The Credit Union will:

- Compare the information in the consumer report to the information obtained from the consumer to verify their identity in accordance with the customer identification procedures.
- Compare the information in the consumer report to the Credit Union's own records such as applications, change of address notifications, or other member account records.
- Compare the information in the consumer report to information obtained from other third party sources.
- Verify the information in the consumer report with the consumer.

The Credit Union will provide accountholders with reasonable means of promptly reporting incorrect address changes:

- Internet
- Telephone
- Written

Confirmation of a member's address may be facilitated by methods as specified in the

Customer Identification – New Accounts subsection, providing the Credit Union a "reasonable belief" that the address is correct. If the Credit Union reasonably believes that the consumer report received relates to the appropriate person and the Credit Union regularly furnishes information to the consumer reporting agency, the Credit Union will furnish the address that the Credit Union has reasonably confirmed to be accurate to the consumer reporting agency. The corrected address should be provided as part of the information regularly furnished to the consumer reporting agency in the reporting period in which the Credit Union establishes a relationship with the consumer.

## Consumer Report Indicates Fraud or Active Duty Alert

A consumer who requests the inclusion of a fraud alert or active duty alert in his or her credit file is exercising a right under the Fair Credit Reporting Act. Consequently, when a credit file contains a fraud or active duty alert, an employee must take reasonable steps to verify the identity of the individual before extending credit, closing an account, or otherwise limiting the availability of credit. The loan officer who pulls a credit report with a fraud or active duty alert must create a record of what steps were taken to verify identity.

When the Credit Union is processing a request for new credit or an increase in an existing credit line and the Credit Union is using a credit report containing an initial fraud, extended fraud, or active duty alert, the Credit Union must contact the member by telephone or must take other reasonable steps to verify the member's identity and confirm the member's credit request is not the result of identity theft. These responsibilities do not apply to Credit Union initiated credit extensions or credit increases.

Where applicable, the following out of wallet questions should be used to verify the identity of a credit applicant. Reference the credit bureau report for correct answers and document the answers given by the applicant.

- What is one of your previous addresses?
- What is the name of a previous employer of yours?
- Where is your mortgage held, and what is the monthly payment?
- Where is your auto loan held, and what is the monthly payment?
- You have a credit card from (fill in the blank); what is the current balance?

If it cannot be confirmed that the request is legitimate, credit will not be extended and the Credit Union will consider whether a SAR should be filed. Concerns should be discussed with supervisors and/or management.

## Consumer Report Unusual Pattern of Activity

Review consumer reports for a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or member 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 was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Because this type of activity is indicative of identity theft, extension of credit must not be granted for individuals whose credit discrepancies cannot be reconciled. Contact the member or applicant and ask out of wallet questions to verify that the person applying for the loan is who they say they are. If you cannot establish a reasonable belief that you know the true identity of the individual, **do not extend credit.**

## Request for Credit/Debit Card Additional/Replacement Card

The Credit Union will not issue an additional or replacement credit/debit card if the request is received within thirty (30) days after the address change notification for that account unless the cardholder is notified of the request at the cardholder's former address or by a previously established method of communication and providing the cardholder a reasonable means of promptly reporting incorrect address changes.

## Request for Additional Authorized Users

When the Credit Union receives a request for the addition of authorized users on the account, the Credit Union will not honor the request unless the identity of the requester has been verified or the Credit Union has reasonable belief that it knows the person's true identity.

## Unexpected Activity on Existing Accounts

Any time the Credit Union suspects there may be a possibility of identity theft because of unexpected activity or transactions, the Credit Union will contact the member to verify the validity of the transaction.

## Mail is Returned as Undeliverable

When mail sent to a member is returned as undeliverable although transactions continue to be conducted in connection with the member's account, the account will be noted and a fee charged.

## Email Messages Returned When Not Sent

When electronic messages are returned to the Credit Union mail servers that were not originally sent by the Credit Union, the IT Department will review the returned emails for possible phishing/pharming attacks. The IT Department will coordinate with the Marketing Department to update the Credit Union website to alert the membership to the fake email. The IT Department will coordinate with its IT vendors to shut down the phishing site.

## Certain Employee Activities Encountered

When an employee has been added as an authorized user to an account, the Credit Union will contact the primary member to confirm that the employee is joint owner. If the employee is not a joint owner, report this to the employee's manager or Director of Human Resources. The Compliance Officer will determine whether a SAR should be filed.

When an employee has accessed or downloaded an unusually large number of member account records, the Director of Human Resources will confront the employee, determine and take appropriate action up to and including dismissal, and consider filing an SAR.

## Unauthorized Attempts to Access an Account

When the Credit Union detects attempts to access a member's account by an unauthorized individual/individuals, contact the member, consider a close and reopen on the member's account, and consider filing a SAR.

When the Credit Union detects, or is informed of, unauthorized access to a member's personal information, the Credit Union employee who receives this information will do the following:

- Close account and reopen with new number.
- Block plastics and reissue.
- Place control flag on the account.
- Refund money lost to fraudulent activity.
- Encourage the member to monitor their credit bureau reports

## Unusually Large or Frequent Check Orders Received

Confirm the order with the member before processing.

## Credit Freeze Encountered

When the person opening an account is unable to lift a credit freeze placed on his or her consumer report, work with the member and the consumer reporting agency to determine the reason for the freeze. Circumstances will determine what other action is taken (close and reopen, etc.).

## Recordkeeping

A record of identity verification will be maintained by the Credit Union. This includes the following:

- A copy or record of any document relied upon for identification.
- A description of the methods and the results of any means used to verify a member's identity.
- A description of the resolution of any substantive discrepancy discovered when the Credit Union verifies identification.

## Record Retention

The Credit Union will retain information about a member (documents obtained from the member, method and results of non-documentary identity verification, and resolution of any discrepancies revealed from identity verification) for five years after the date the account is closed. For credit card accounts, the retention period is five years after the date the account is closed or becomes dormant.

## Notice of Identity Verification

The Credit Union will provide members notice that the Credit Union is requesting information to verify their identity. This notice may be provided orally, in written, or in electronic form. If the Credit Union provides the notice in writing, it may be provided with other information posted in the Credit Union lobby or provided with other disclosures required by law. The notice will contain the following or similar language:

**USA PATRIOT ACT - NOTICE**

**Important Information about Procedures for Opening a New Account:**
To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.

## Privacy Protection

The Credit Union will maintain a written Privacy Protection Policy that addresses privacy and information handling for all sensitive data held by the Credit Union, including

information gathered from its website. The Privacy Protection Policy will be included in Credit Union literature and displayed on the Credit Union website.

### Training

Employees will be trained on identity theft red flag awareness at least annually. This training may be included in other training such as new employee, information security, etc. when appropriate.

### Oversight of Service Provider Arrangements

Whenever the Credit Union engages a service provider to perform an activity in connection with one or more covered accounts, the Credit Union will take steps to ensure that the service provider's activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Relevant red flags will be identified and procedures will be established that either require the service provider to report the red flag to the Credit Union or require the service provider to take appropriate steps to prevent or mitigate identity theft.

## INDEX

## Historical Record of Policy Changes

**Date Revised:** March 2009
**Date Ratified:**

Program Administration
*New Section*

Credit/Debit Cards
*New Section*

Credit Bureau Reports
*New Section*

---

**Date Revised:** July 2010
**Date Ratified:** August 2010

Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies
*New Section*

---

**Date Rewritten:** July 2013
**Date Ratified:** July 2013