
Compliance Essentials
Identity Theft Red Flag Guidelines
UTAH'S CREDIT UNIONS

Overview

Overview

- Credit Unions are required to develop and implement written identity theft prevention programs “ID Theft Red Flag Rules.”
- The Red Flags Rules are part of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.
- Under these Rules, credit unions with covered accounts must have identity theft prevention programs in place to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

Overview

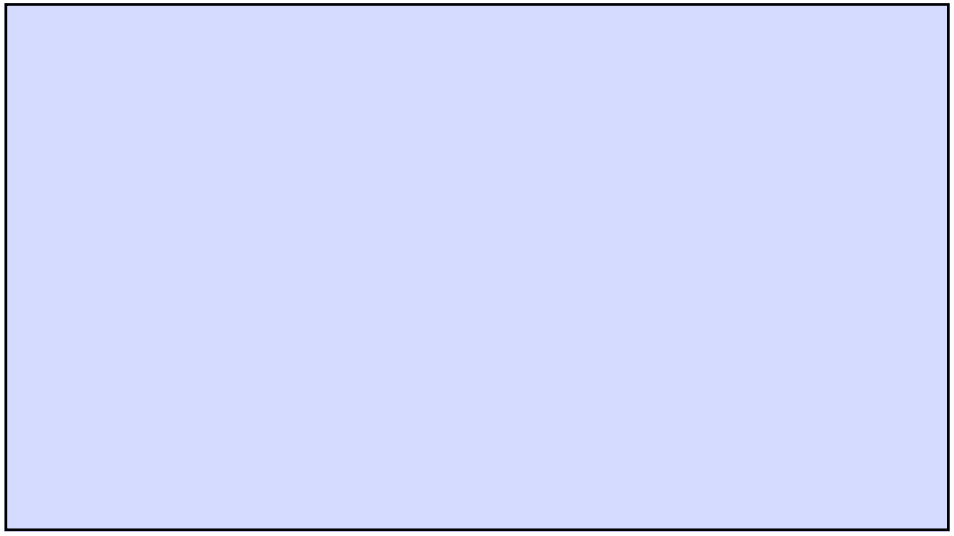
- Credit Unions are required to develop and implement written identity theft prevention programs “ID Theft Red Flags.”
- The Red Flags Rules are part of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.
- Under these Rules, credit unions with covered accounts must have identity theft prevention programs in place to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

Overview

Regulations

- Federal Credit Unions:
  - National Credit Union Administration
  - 12 CFR Part 717, Subpart J: Identity Theft Red Flags
  - 12 CFR Part 717, Appendix J: Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation
- State Chartered Credit Unions:
  - Federal Trade Commission:
  - 16 CFR Part 681: Identity Theft Rules
  - 16 CFR Appendix A: Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

UTAH'S CREDIT UNIONS



Overview

Key Provisions

The credit union must:

1. periodically conduct a risk assessment to determine whether it offers or maintains covered accounts;
2. establish and implement a written Program, appropriate to the credit union's size and complexity and the nature and scope of its activities;
3. include reasonable policies and procedures to:
   a) identify relevant red flags;
   b) detect red flags;
   c) respond appropriately to detected red flags; and
   d) ensure the Program is updated periodically to reflect changes in risks;

UTAH'S CREDIT UNIONS

Overview

Key Provisions

The credit union must:

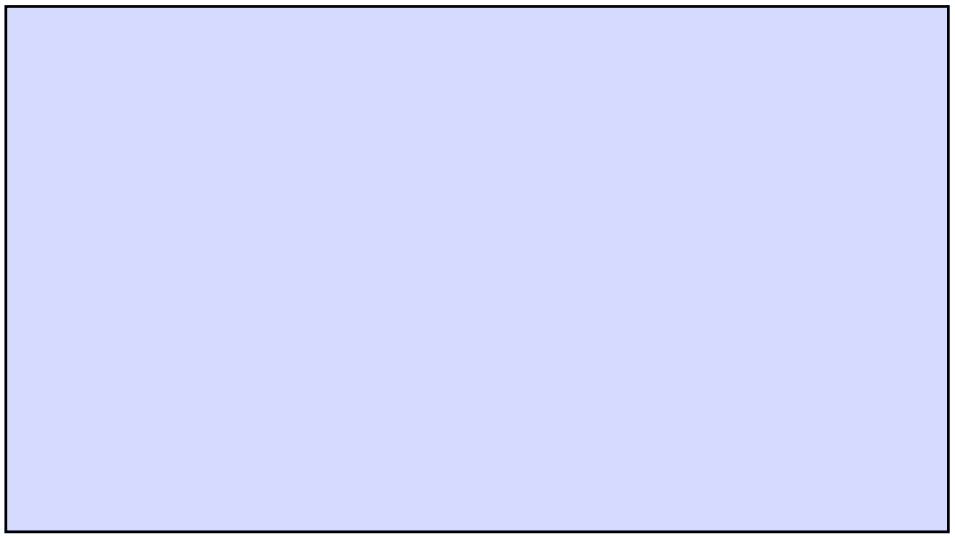
4. provide for continued administration of the Program:
   a) ensure initial proper approval;
   b) ensure senior management involvement;
   c) address staff training; and
   d) ensure service provider oversight; and
5. consider the interagency guidelines

Definitions

Definitions

Covered account:

- An account that a credit union offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, checking account, or share account; and
- Any other account that the credit union offers or maintains for which there is a reasonably foreseeable risk to members or to the safety and soundness of the credit union from identity theft, including financial, operational, compliance, reputation, or litigation risks.



Definitions

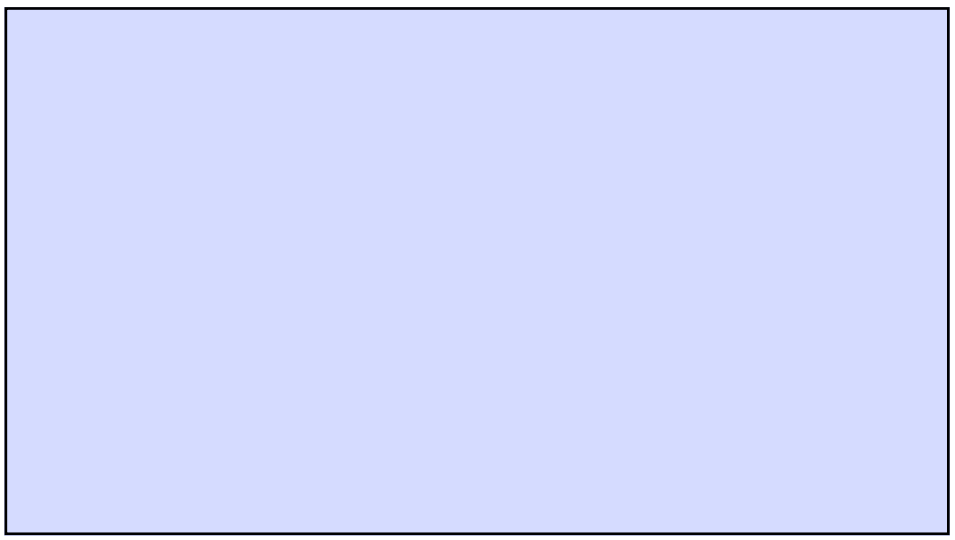
Identity theft: A fraud committed or attempted using the identifying information of another person without authority.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Periodic Identification of Covered Accounts

Periodic Identification of Covered Accounts

- Credit unions must periodically determine whether they offer or maintains covered accounts.
- As a part of this determination, a credit union must conduct a risk assessment to determine whether it offers or maintains covered accounts, taking into consideration:
  1. The methods it provides to open its accounts;
  2. The methods it provides to access its accounts; and
  3. Its previous experiences with identity theft.



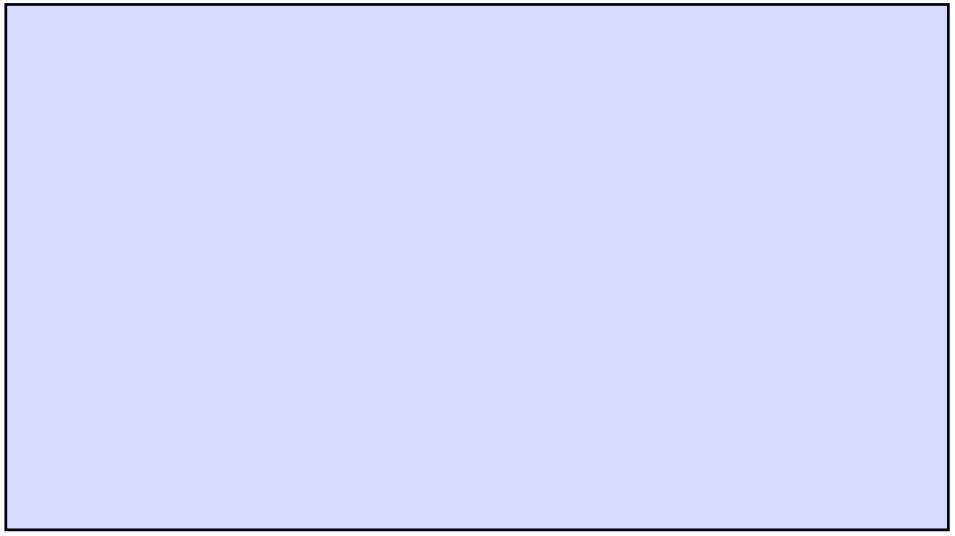
Establishment of an Identity Theft Prevention Program

Establishment of an Identity Theft Prevention Program

Program Requirement

- Each credit union that offers covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.
- The Program must be appropriate to the size and complexity of the credit union and the nature and scope of its activities.

UTAH'S CREDIT UNIONS



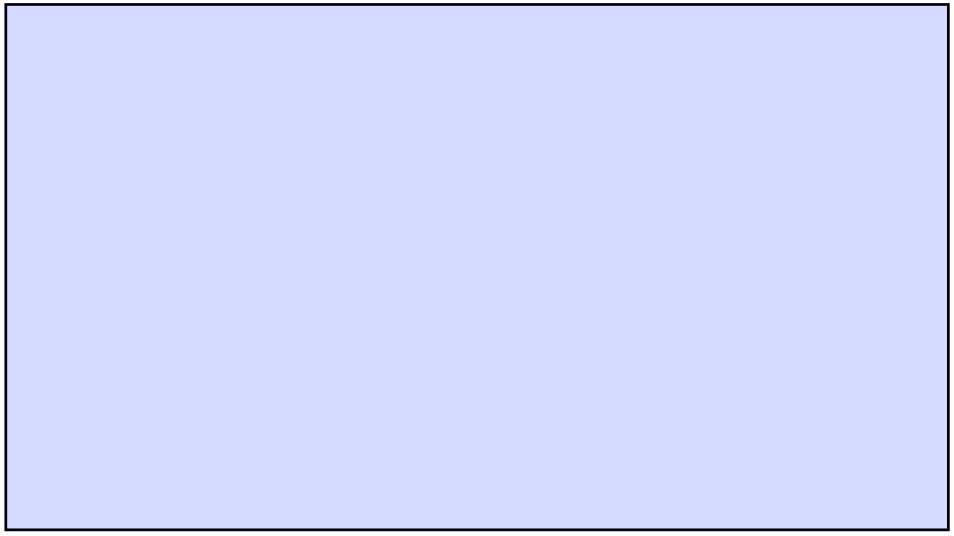
Establishment of an Identity Theft Prevention Program

Elements of the Program

The Program must include reasonable policies and procedures to:

- Identify relevant Red Flags for the covered accounts that the credit union offers or maintains, and incorporate those Red Flags into its Program;
- Detect Red Flags that have been incorporated into the Program
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft
- Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to members and to the safety and soundness of the credit union from identity theft.

UTAH'S CREDIT UNIONS



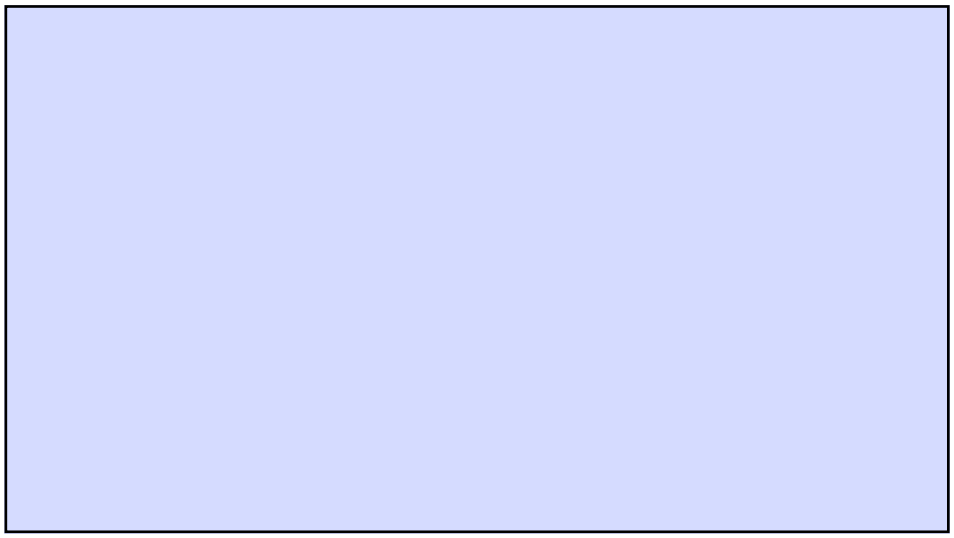
Establishment of an Identity Theft Prevention Program

Administration of the Program

A credit union must provide for the continued administration of the Identity Theft Prevention Program and must:

1. Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;
2. Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;
3. Train staff, as necessary, to effectively implement the Program; and
4. Exercise appropriate and effective oversight of service provider arrangements.

UTAH'S CREDIT UNIONS



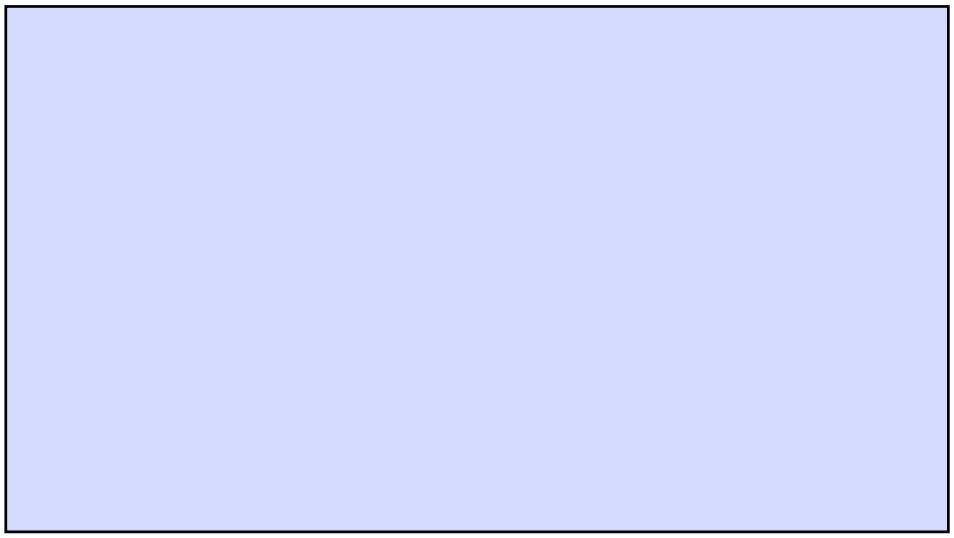
Duties of card issuers regarding changes of address

Duties of card issuers regarding changes of address

Definitions

Cardholder: A member who has been issued a credit or debit card.

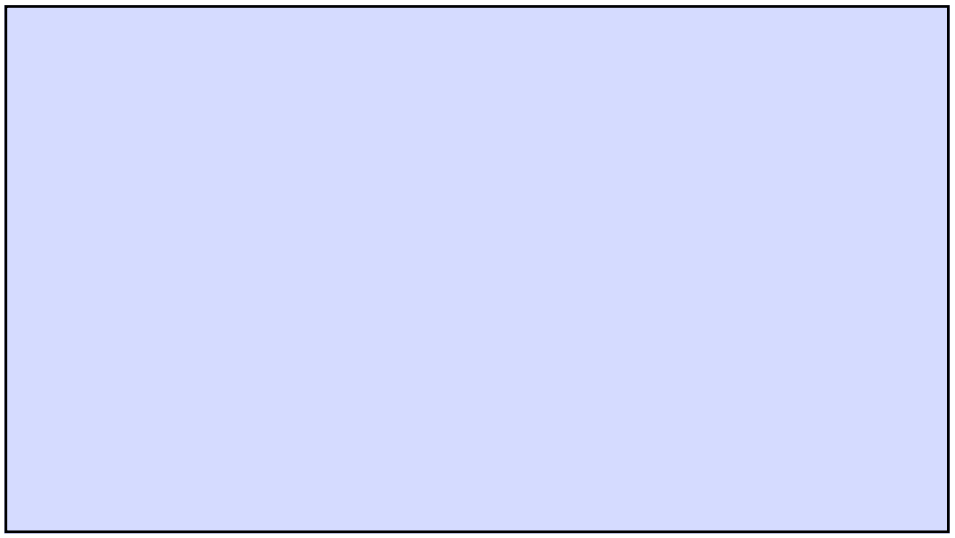
Clear and conspicuous: Reasonably understandable and designed to call attention to the nature and significance of the information presented.



Duties of card issuers regarding changes of address

Address validation requirements

- A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a member's debit or credit card account and,
- Within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account.



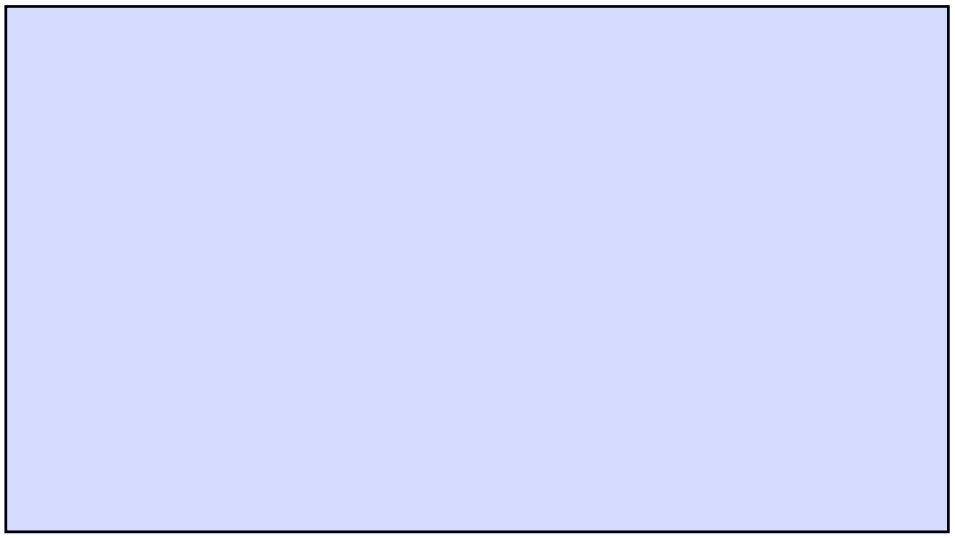
Duties of card issuers regarding changes of address

Address validation requirements

A card issuer may not issue an additional or replacement card unless specific procedures are followed

Option 1:

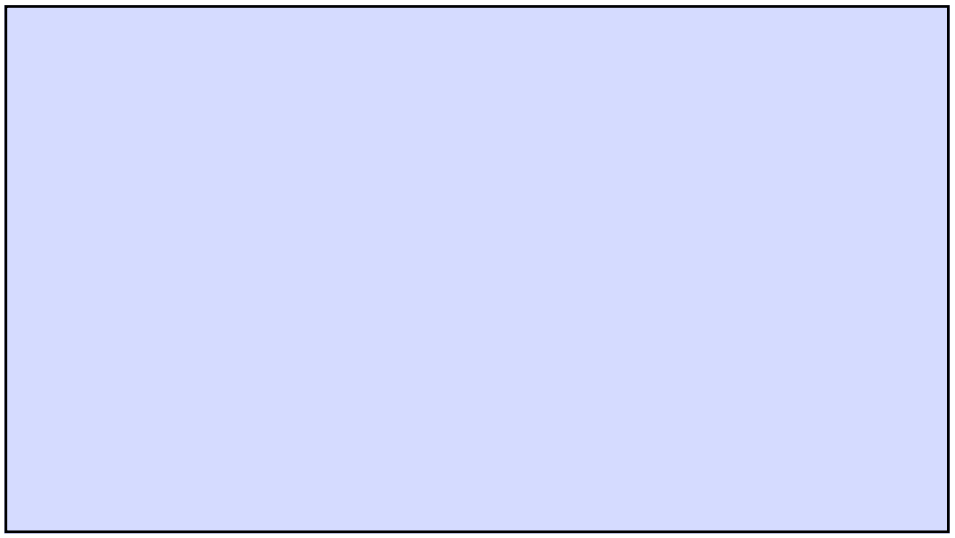
1. Notify the cardholder of the request
   A. At the cardholder's former address; or
   B. By any other means of communication that the card issuer and the cardholder have previously agreed to use; and
2. Provides to the cardholder a reasonable means of promptly reporting incorrect address changes



Duties of card issuers regarding changes of address

Address validation requirements

Option 2: Otherwise assesses the validity of the change of address in accordance with the credit union's ID Theft Red Flag Program



Duties of card issuers regarding changes of address

- **Alternative timing of address validation:** A card issuer may satisfy the requirements if it validates an address pursuant Option 1 or Option 2 when it receives an address change notification, before it receives a request for an additional or replacement card.
- **Form of notice:** Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

UTAH'S CREDIT UNIONS

Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

- The guidelines are intended to assist credit unions in the formulation and maintenance of an Identity Theft Prevention Program
- In designing its Program, a credit union may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to members or to the safety and soundness of the credit union from identity theft.

Identifying Relevant Red Flags

1. **Risk Factors.** A credit union should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:
   - The types of covered accounts it offers or maintains;
   - The methods it provides to open its covered accounts;
   - The methods it provides to access its covered accounts; and
   - Its previous experiences with identity theft.

UTAH'S CREDIT UNIONS

Identifying Relevant Red Flags

2. **Sources of Red Flags.** Credit unions should incorporate relevant Red Flags from sources such as:
   - Incidents of identity theft that the credit union has experienced;
   - Methods of identity theft that the credit union has identified that reflect changes in identity theft risks; and
   - Applicable supervisory guidance.

UTAH'S CREDIT UNIONS

Identifying Relevant Red Flags

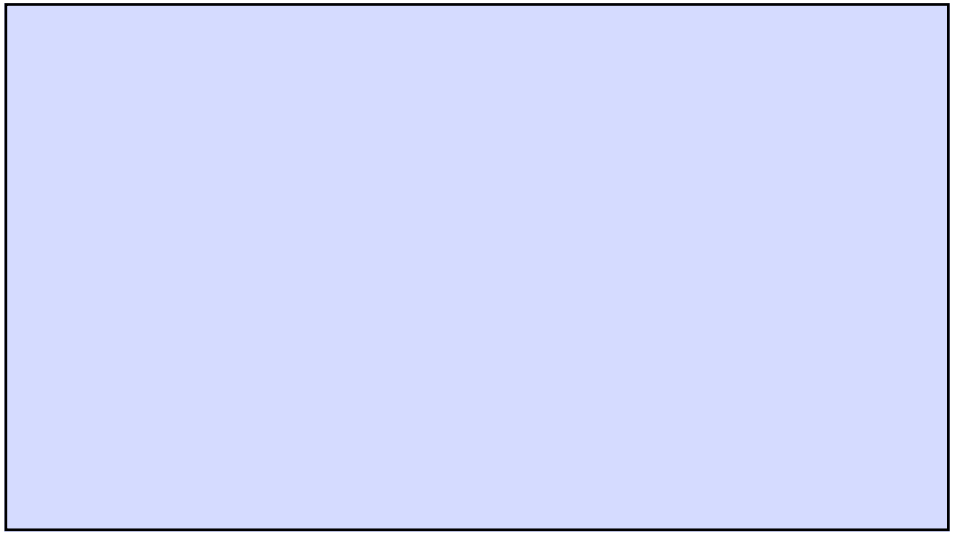
3. **Categories of Red Flags.** The Program should include relevant Red Flags from the following categories, as appropriate.
   - Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
   - The presentation of suspicious documents;
   - The presentation of suspicious personal identifying information, such as a suspicious address change;
   - The unusual use of, or other suspicious activity related to, a covered account; and
   - Notice from members, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the credit union.

Categories of Red Flags

Alerts, Notifications or Warnings From a Consumer Reporting Agency

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy
- 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; or
  - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

UTAH'S CREDIT UNIONS



Categories of Red Flags

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- 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 information provided by the person opening a new covered account or member presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the credit union, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Categories of Red Flags

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the credit union. For example:
  - The address does not match any address in the consumer report; or
  - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- Personal identifying information provided by the member is not consistent with other personal identifying information provided by the member. For example, there is a lack of correlation between the SSN range and date of birth.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the credit union. For example:
  - The address on an application is the same as the address provided on a fraudulent application; or
  - The phone number on an application is the same as the number provided on a fraudulent application.

UTAH'S CREDIT UNIONS

Categories of Red Flags

Suspicious Personal Identifying Information

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the credit union. For example:
  - The address on an application is fictitious, a mail drop, or prison; or
  - The phone number is invalid, or is associated with a pager or answering service.
- The SSN provided is the same as that submitted by other persons opening an account or other members.
- The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or by other members.

UTAH'S CREDIT UNIONS

Categories of Red Flags

Suspicious Personal Identifying Information

- The member fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the credit union.
- For credit unions that use challenge questions, the person opening the covered account or the member cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Categories of Red Flags

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

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:
  - The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
  - The member fails to make the first payment or makes an initial payment but no subsequent payments.

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

- Nonpayment 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

UTAH'S CREDIT UNIONS

Categories of Red Flags

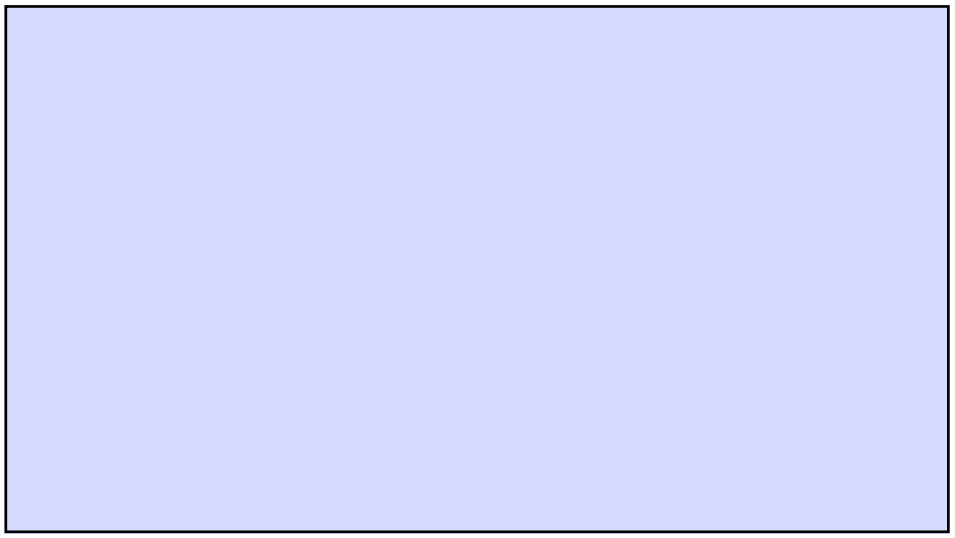
Unusual Use of, or Suspicious Activity Related to, the Covered Account

- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- Mail sent to the member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member's covered account.
- The credit union is notified that the member is not receiving paper account statements.
- The credit union is notified of unauthorized charges or transactions in connection with a member's covered account.

Categories of Red Flags

Notice From Members, Victims of Identity Theft, Law Enforcement Authorities, or Others

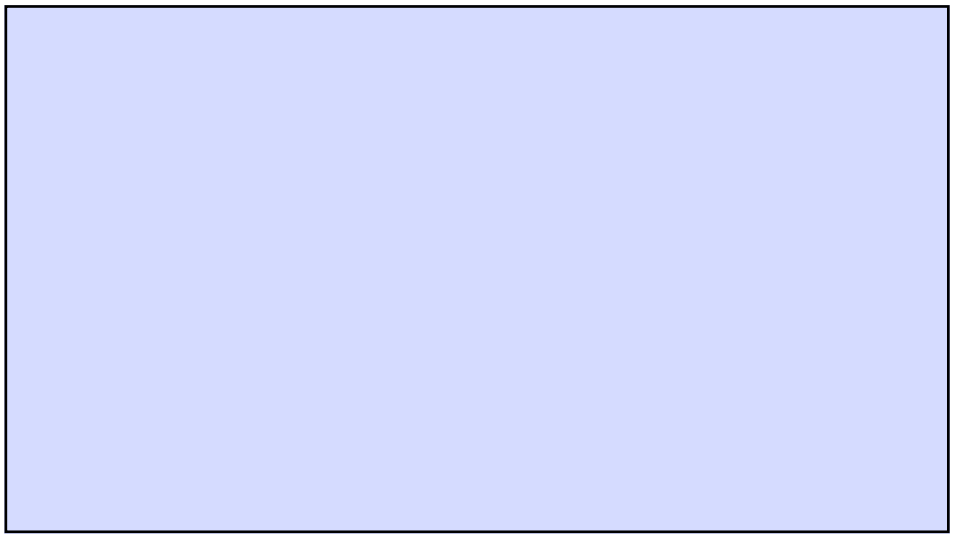
- The credit union is notified by a member, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.



Detecting Red Flags

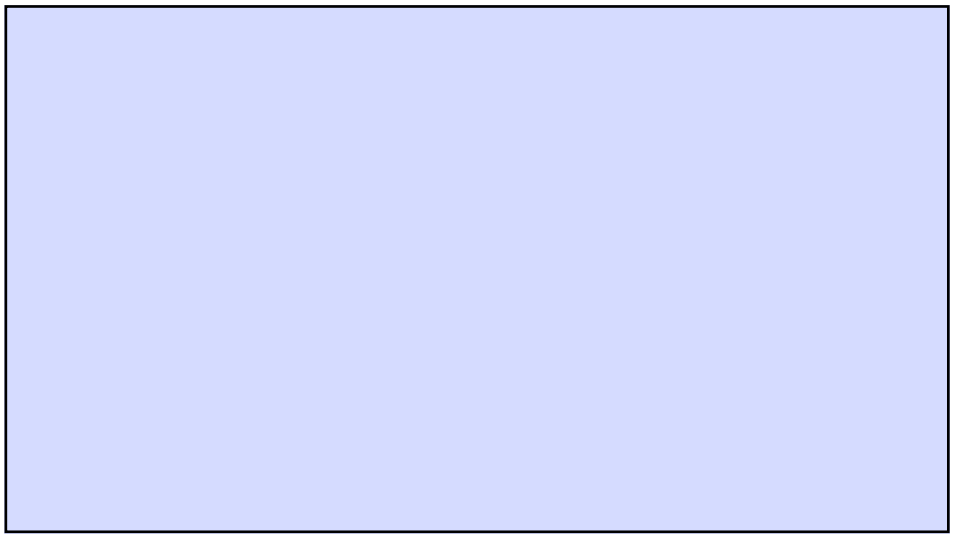
The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account; for example, using the policies and procedures regarding identification and verification under the credit union's Customer Identification Program
- Authenticating members, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.



Preventing and Mitigating Identity Theft

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



Preventing and Mitigating Identity Theft

Appropriate responses may include the following:

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

UTAH'S CREDIT UNIONS

Updating the Program

Credit unions should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to members or to the safety and soundness of the credit union from identity theft, based on factors such as:

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

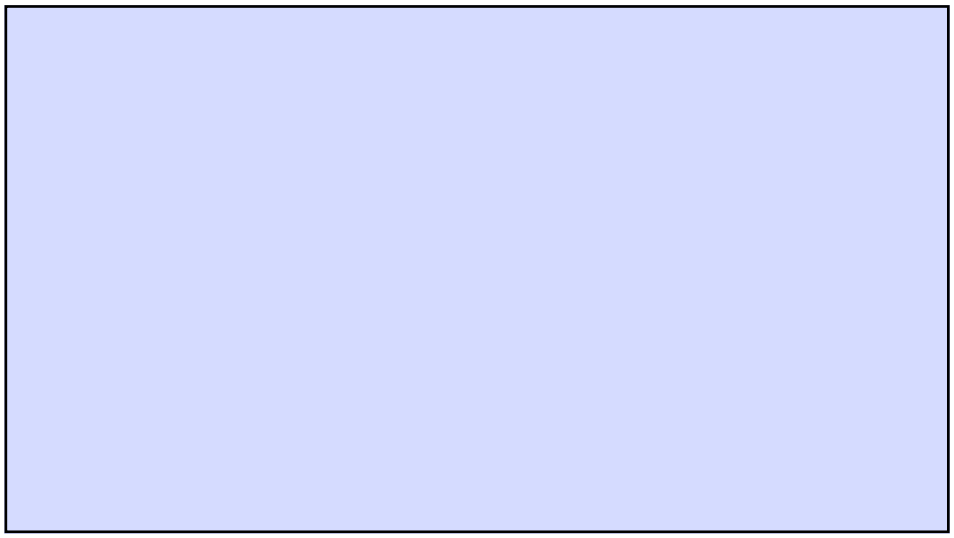
UTAH'S CREDIT UNIONS

Methods for Administering the Program

Oversight of Program

Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

- Assigning specific responsibility for the Program's implementation
- Reviewing reports prepared by staff regarding compliance
- Approving material changes to the Program as necessary to address changing identity theft risks.

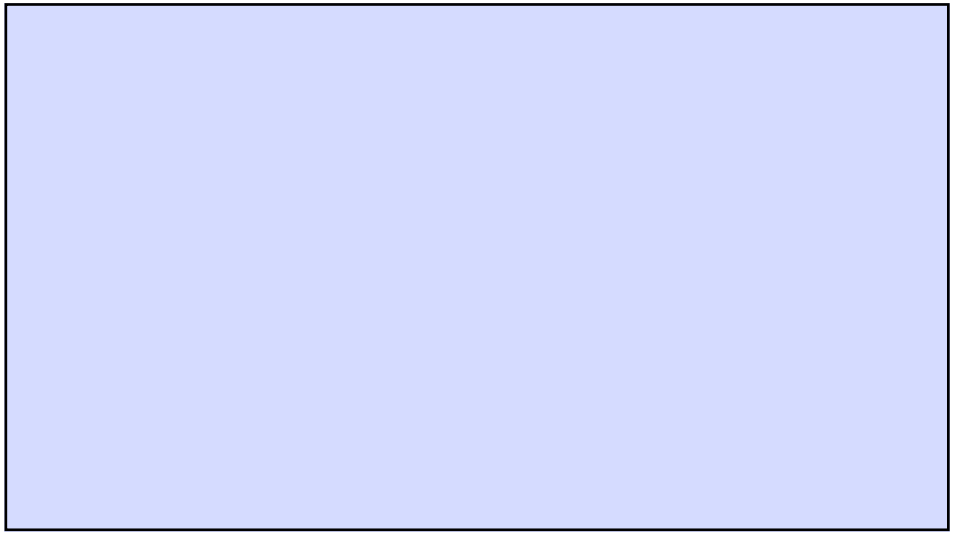


Methods for Administering the Program

Reports

- Staff of the credit union responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually regarding compliance with the program
- The report should address material matters related to the Program and evaluate issues such as:
  - the effectiveness of the policies and procedures of the credit union in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts
  - service provider arrangements
  - significant incidents involving identity theft and management's response
  - recommendations for material changes to the Program

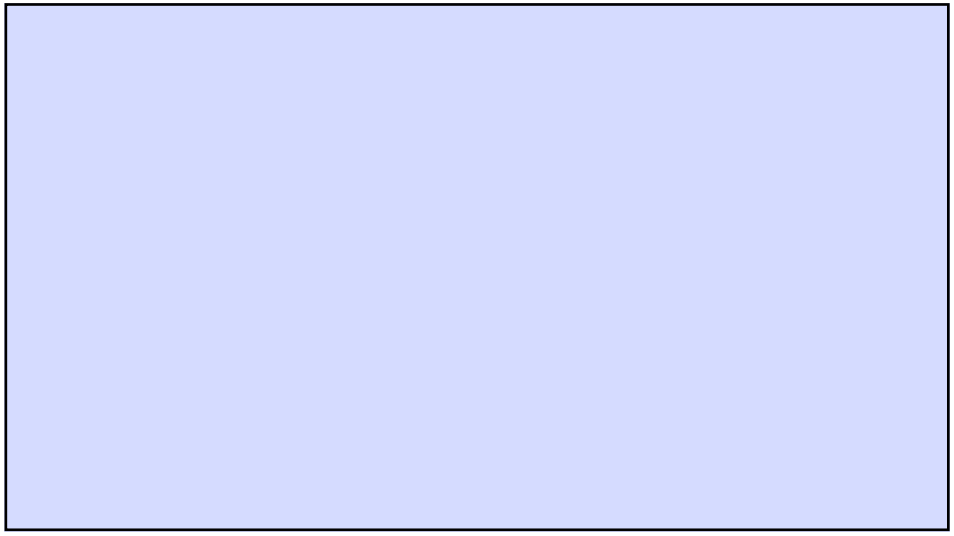
UTAH'S CREDIT UNIONS



Oversight of service provider arrangements

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

UTAH'S CREDIT UNIONS

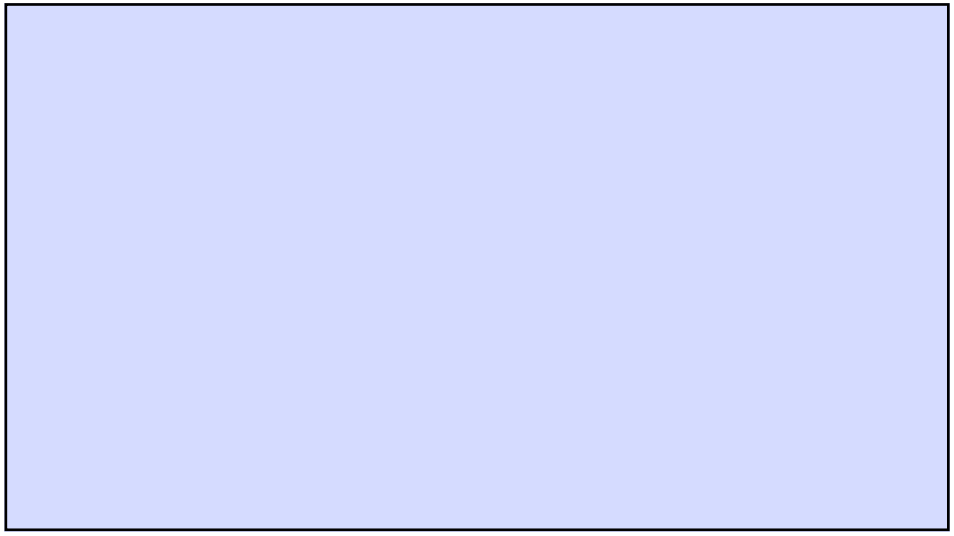


Other Applicable Legal Requirements

Credit unions should be mindful of other related legal requirements that may be applicable, such as:

- Filing a Suspicious Activity Report
- Addressing circumstances under which credit may be extended when the credit union detects a fraud or active-duty alert
- Implementing any requirements regarding furnishing information to credit reporting agencies to correct or update inaccurate or incomplete information, and to not report information that the credit union has reasonable cause to believe is inaccurate; and
- Complying with the prohibitions on the sale, transfer, and placement for collection of certain debts resulting from identity theft

UTAH'S CREDIT UNIONS



Questions?

Heather Line
Compliance Specialist
heather@utahscreditunions.org
801-599-2168

Coming Soon

- Thursday March 21, 2024: Privacy and Information Security
- Thursday April 11, 2024: Regulation CC, Twice (Rescheduled)