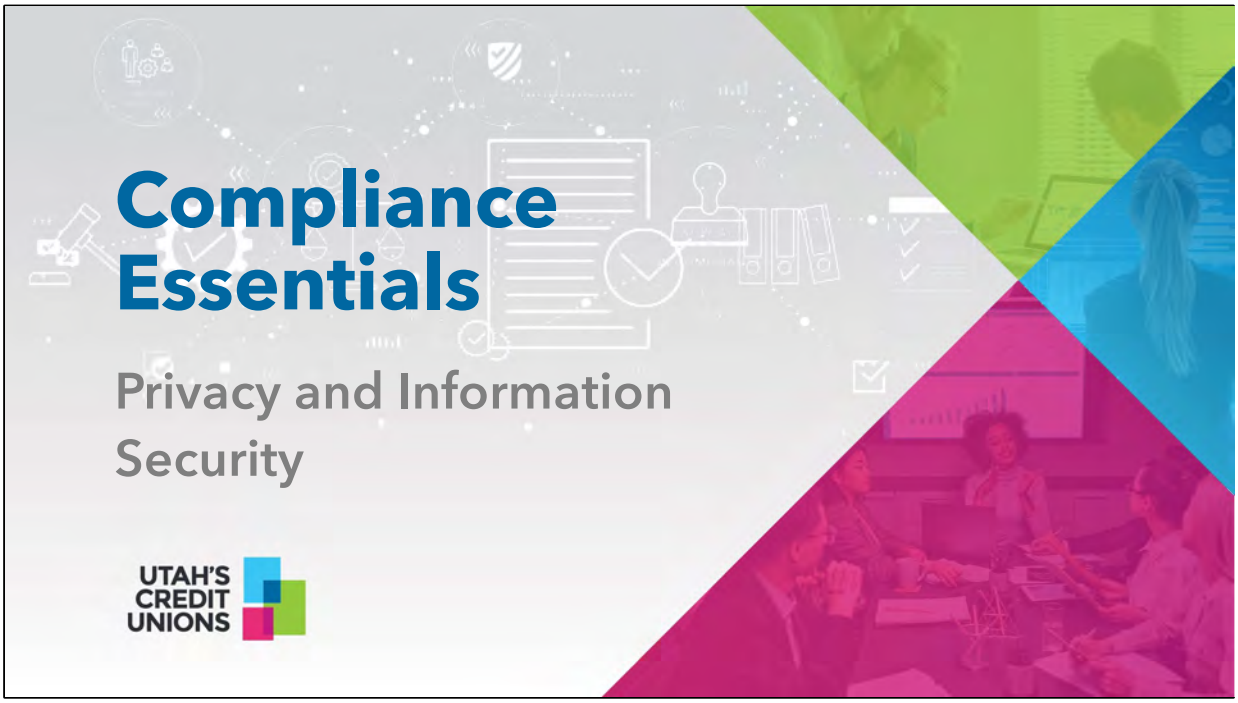
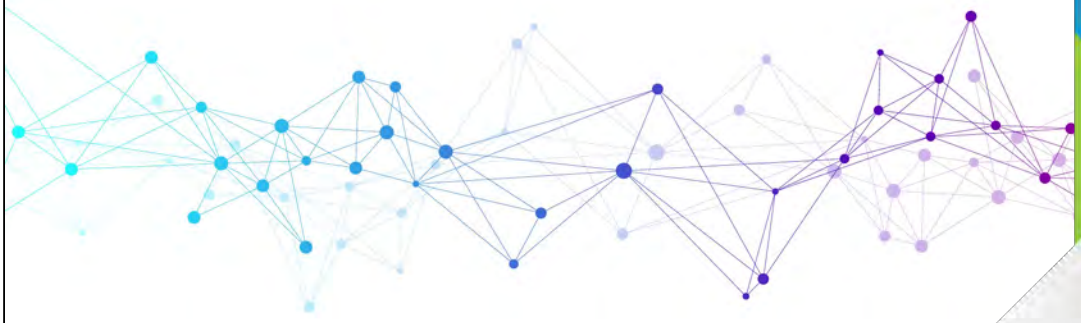

Compliance Essentials
Privacy and Information Security
UTAH'S CREDIT UNIONS

Privacy of Consumer Financial Information



UTAH'S CREDIT UNIONS

Introduction

- The CFPB regulation is found at 12 CFR 1016
- Addresses disclosure of nonpublic personal information (NPPI) about members

General Rules

- Disclosures to members are required before a credit union can share information with businesses outside of the credit union (privacy notice).
- Credit unions are forbidden from providing an account number or similar access number for a credit card account, share account, or transaction account of any consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing efforts.
- Before a credit union can share information with a nonaffiliated third party for marketing purposes, the credit union must give members a reasonable opportunity to request that the information not be shared (opt-out).
- NPPI can be shared with nonaffiliated third parties without providing an opt-out to the member under certain exceptions.

Definitions

Member

For purposes of the privacy regulation, a member or a person with a "member relationship" is a consumer who has a continuing relationship with the credit union. Examples include:

- A member as defined in the credit union's bylaws
- A nonmember who has a share, share draft, credit card account, or other loan jointly with a member
- A nonmember who has a loan serviced by the credit union
- A nonmember served by an NCUA-designated low-income credit union

UTAH'S CREDIT UNIONS

Definitions

Consumer

An individual who obtains or has obtained a financial product or service from the credit union, that is to be used primarily for personal, family, or household purposes

Personally Identifiable Financial Information

Information that an individual provides to a credit union in order to obtain a product or service, or that results from any transaction between the credit union and the member

Definitions

Nonpublic Personal Information

Any personally identifiable financial information about a member that the credit union possesses

Publicly Available Information

Information that the credit union has a reasonable basis to believe is lawfully made available to the general public (such as from government records or widely distributed media such as telephone listings)

Disclosures

- The credit union must provide initial and annual (exceptions apply) privacy disclosure notices to all individuals who receive services from the credit union for personal or household use.
- Joint accountholders do not need to receive a separate copy of the privacy and opt out notices.
- The credit union is not required to provide separate notices to nonmember individuals who are co-borrowers, co-makers, or guarantors unless the credit union will share NPPI not covered by an exception.
- The credit union must provide initial disclosures for new member relationships and annually ("once every 12 months") after the initial notices are given (exceptions apply).

Initial Notice

Provide the initial notice:

- Not later than when the person becomes a member of the credit union
- Not later than when a nonmember receives any credit union services

One Time Notice

Required if the credit union chooses to provide NPPI to third parties for marketing purposes about a person who is not a member of the credit union but uses the credit union's services

Annual Notice

- Is only required under certain circumstances
- Must be written in a form that can be retained
- Can be mailed with other credit union material
- Cannot be provided as a general advertisement or merely posted in the credit union's lobby
- Must be "clear and conspicuous"

Annual Notice

Annual Notice Not Required

In 2015, the Gramm-Leach-Bliley Act was amended to eliminate the requirement that credit unions send an annual privacy notice to its members under certain conditions. In order to qualify for the exemption, credit unions must:

- Share non-public personal information with non-affiliated third parties only in accordance with one of the exceptions provided for in Regulation P; and
- Not have changed its privacy policies and practices since the last time it provided an annual privacy notice to members.

Standardized Privacy Notice

- Available as a fill-in form: https://www.federalreserve.gov/bankinforeg/privacy_notice_instructions.pdf
- The standardized form replaced the model language or sample clauses in the regulation that most credit unions were using in their privacy notices.
- Credit unions using the model form will be deemed to have satisfied the content requirements for Privacy notices and therefore granted a safe harbor with regard to Privacy compliance.
- Safe harbor protection is no longer available for model clauses.
- Use of the standard form is voluntary.

Notice Content

- The categories of nonpublic personal information the credit union collects.
- The categories of nonpublic personal information the credit union discloses.
- The categories of affiliates and nonaffiliated third parties to whom the credit union discloses nonpublic personal information.
- The categories of nonpublic personal information about former members that the credit union discloses and to whom.
- If the credit union discloses nonpublic personal information to third-party servicers and other financial institutions with which the credit union has joint marketing agreements, a separate statement of the categories of information disclosed and the types of third parties this information is shared with
- An explanation of the consumer/member's right to opt-out and how to exercise the right to opt out, if applicable.
- The application of opt-out rights under the Fair Credit Reporting Act, if applicable.
- The credit union's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.
- The language required for any disclosures made to transaction processors or with the member's consent: "disclosures to other nonaffiliated parties as permitted by law."

UTAH'S CREDIT UNIONS

Simplified Notice

If a credit union does not anticipate disclosing information to affiliates or nonaffiliated third parties for marketing purposes, the credit union can provide a "simplified notice." This notice will require the credit union to disclose:

1. The categories of information collected.
2. The credit union's policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information.
3. The statement of "disclosures to other nonaffiliated third parties as permitted by law."
4. Opt-out notice for nonmember consumers, if applicable.

Revised Privacy Notices

- A credit union cannot disclose any NPPI about a member to a nonaffiliated third party unless the arrangement is properly described in the most recent disclosure made.
- If circumstances change on the information collected and/or disclosed, the credit union may have to distribute an updated privacy notice (and possible opt-out notice) before the disclosure can be made.

Opt-out Notice

When applicable, the credit union must provide a conspicuous notice that explains the right of the person whose NPPI is going to be shared with certain nonaffiliated parties to "opt out," and must provide a reasonable means by which and a reasonable time in which the person may exercise the opt-out right.

Contents

- All categories of nonpublic personal information that the credit union discloses or reserves the right to disclose
- The financial products or services the consumer obtains which the opt-out direction would apply to. The credit union can allow the consumer/member to exercise a "partial opt-out".

Opt-out Notice

Opt-Out Methods

Acceptable methods to provide for the opt-out include:

- Toll-free number
- Internet
- Mail-in form (the initial or annual notice must accompany the form)

Opt-Out Timing

- The credit union must give the consumer "a reasonable opportunity" to opt out before NPPI is shared with a nonaffiliated third party. Thirty days is generally seen as "reasonable"
- The credit union must comply with the consumer's opt-out direction "as soon as reasonably practicable" after the credit union receives the notice.
- The consumer/member can exercise his right to opt out at any time, and the opt-out direction remains in place until revoked in writing by that person.

UTAH'S CREDIT UNIONS

Opt-out Notice

Joint Accountholders

The opt out notice must explain how the credit union will treat an opt-out direction by one or more of the joint account holders. The credit union can choose to:

- Treat an opt-out direction by any one of the joint accountholders to apply to everyone on the account
- Permit each joint accountholder to opt out separately.

Exceptions to the General Privacy Notice and Opt-Out Rules

Affiliates

- Generally will be CUSOs
- A credit union can share information with an affiliate without having to give the person the opportunity to opt out unless that sharing triggers protections under the FCRA.
- A credit union can share account numbers with an affiliate.
- A credit union and its affiliate can send out a joint privacy notice as long as the notice accurately reflects information for all credit unions and affiliates represented on the disclosure.

Exceptions to the General Privacy Notice and Opt-Out Rules

Nonaffiliated Third-party Financial Institutions

- Credit unions are permitted to share NPPI with nonaffiliated financial institutions with whom the credit union has a joint marketing agreement without giving an opt-out.
- A "joint agreement" means a written contract the credit union has with another financial institution where the parties jointly offer, endorse, or sponsor a financial product or service.
- The contract must contain provisions requiring confidentiality and forbidding use by the third party of the information for anything other than what is provided in the contract.

UTAH'S CREDIT UNIONS

Exceptions to the General Privacy Notice and Opt-Out Rules

Nonaffiliated Third Parties that Perform Services for the Credit Union

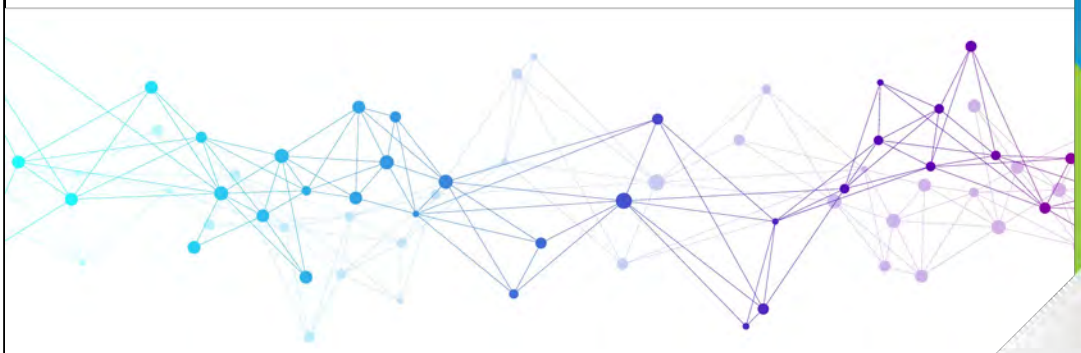
- Credit Unions may share NPPI with nonaffiliated third parties that the credit union contracts to perform services on its behalf without providing and opt-out. For example, a company that prints and mails the credit union's statements.
- There must be a formal agreement requiring confidentiality and forbidding reuse of the information by the third party.

UTAH'S CREDIT UNIONS

Fair Credit Reporting

- Under the Fair Credit Reporting Act (FCRA) credit unions may share with affiliates "experience" information about its members without limitation.
- Any other information may also be shared among affiliated institutions if:
  - The member receives a clear and conspicuous disclosure that the information may be shared among the affiliates
  - The member is given an opportunity to opt out of the sharing before it takes place

Information Security



UTAH'S CREDIT UNIONS

Introduction

- Guidelines found in NCUA rule 748, Appendix A
- “Guidelines for Safeguarding Member Information”
- Also part of the GLBA

Introduction

- Guidelines provide guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information.
- Guidelines also address standards with respect to the proper disposal of consumer information

Standards for Safeguarding Member Information

Information Security Program

- A comprehensive written information security program includes administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities.
- While all parts of the credit union are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

UTAH'S CREDIT UNIONS

Standards for Safeguarding Member Information

Objectives

A credit union's information security program should be designed to:

- Ensure the security and confidentiality of member information
- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member
- Ensure the proper disposal of member information and consumer information

Development and Implementation of Member Information Security Program

Involve the Board of Directors

The board of directors or an appropriate committee of the board of each credit union should:

- Approve the credit union's written information security policy and program; and
- Oversee the development, implementation, and maintenance of the credit union's information security program, including:
  - Assigning specific responsibility for its implementation and
  - Reviewing reports from management

UTAH'S CREDIT UNIONS

Development and Implementation of Member Information Security Program

Assess Risk

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information; and
3. Assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.

Development and Implementation of Member Information Security Program

Manage and Control Risk

The information security program should be designed to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the credit union's activities.

Each credit union must consider whether the following security measures are appropriate for the credit union and, if so, adopt those measures the credit union concludes are appropriate:

Development and Implementation of Member Information Security Program

Manage and Control Risk

A. Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

B. Access restrictions at physical locations containing member information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

C. Encryption of electronic member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

D. Procedures designed to ensure that member information system modifications are consistent with the credit union's information security program;

UTAH'S CREDIT UNIONS

Development and Implementation of Member Information Security Program

Manage and Control Risk

E. Dual controls procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information;

F. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems;

G. Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies; and

H. Measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures.

UTAH'S CREDIT UNIONS

Development and Implementation of Member Information Security Program

Manage and Control Risk

Other requirements:

- Train staff to implement the credit union's information security program.
- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.
- Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of member information and consumer information

UTAH'S CREDIT UNIONS

Development and Implementation of Member Information Security Program

Oversee Service Provider Arrangements

Exercise appropriate due diligence in selecting its service providers

- Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines; and
- Where indicated by the credit union's risk assessment, monitor its service providers to confirm that they have satisfied their obligations
- As part of this monitoring, a credit union should review audits, summaries of test results, or other equivalent evaluations of its service providers.

UTAH'S CREDIT UNIONS

Development and Implementation of Member Information Security Program

Adjust the Program

Each credit union should monitor, evaluate, and adjust, as appropriate, the information security program in light of any:

- Relevant changes in technology
- The sensitivity of its member information
- Internal or external threats to information, and
- The credit union's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to member information systems.

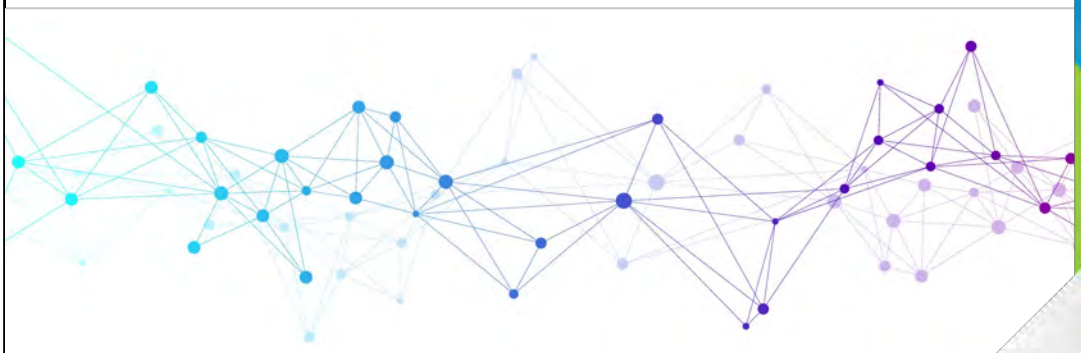
Development and Implementation of Member Information Security Program

Report to the Board

- Each credit union should report to its board or an appropriate committee of the board at least annually.
- This report should describe the overall status of the information security program and the credit union's compliance with these guidelines.
- The report should discuss:
  - Material matters related to its program
  - Risk assessment
  - Risk management and control decisions
  - Service provider arrangements
  - Results of testing
  - Security breaches or violations and management's responses
  - Recommendations for changes in the information security program

UTAH'S CREDIT UNIONS

Response Programs



UTAH'S CREDIT UNIONS

Introduction

- Guidance found in NCUA rule 748, Appendix B
- "Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice"
- Also part of the GLBA

Introduction

- Guidance found in NCUA rule 748, Appendix B
- "Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice"
- Also part of the GLBA
- Describes response programs, including member notification procedures, that a credit union should develop and implement to address unauthorized access to or use of member information that could result in substantial harm or inconvenience to a member.

Introduction

- Every credit union should develop and implement a risk-based response program to address incidents of unauthorized access to member information in member information systems
- A response program should be a key part of a credit union's information security program.
- The program should be appropriate to the size and complexity of the credit union and the nature and scope of its activities.

Introduction

- Each credit union should also be able to address incidents of unauthorized access to member information in member information systems maintained by its service providers.
- A credit union's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to or use of the credit union's member information, including notification of the credit union as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

Components of a Response Program

1. At a minimum, a credit union's response program should contain procedures for the following:
   a) Assessing the nature and scope of an incident, and identifying what member information systems and types of member information have been accessed or misused;
   b) Notifying the appropriate NCUA Regional Director, and, in the case of state-chartered credit unions, its applicable state supervisory authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information
   c) Notifying appropriate law enforcement authorities, in addition to filing a timely SAR
   d) Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of member information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and
   e) Notifying members when warranted

Components of a Response Program

2. Where an incident of unauthorized access to member information involves member information systems maintained by a credit union's service providers, it is the responsibility of the credit union to notify the credit union's members and regulator. However, a credit union may authorize or contract with its service provider to notify the credit union's members or regulators on its behalf.

Member Notice

1. Credit unions have an affirmative duty to protect their members' information against unauthorized access or use. Notifying members of a security incident involving the unauthorized access or use of the member's information in accordance with the standard set forth below is a key part of that duty.

2. Timely notification of members is important to manage a credit union's reputation risk. Effective notice also may reduce a credit union's legal risk, assist in maintaining good member relations, and enable the credit union's members to take steps to protect themselves against the consequences of identity theft. When member notification is warranted, a credit union may not forgo notifying its customers of an incident because the credit union believes that it may be potentially embarrassed or inconvenienced by doing so.

Member Notice

Standard for Providing Notice

- When a credit union becomes aware of an incident of unauthorized access to sensitive member information, the credit union should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.
- If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible.
- Member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay.
- However, the credit union should notify its members as soon as notification will no longer interfere with the investigation.

UTAH'S CREDIT UNIONS

Member Notice

Standard for Providing Notice

- A credit union must protect against unauthorized access to or use of member information that could result in substantial harm or inconvenience to any member.
- Substantial harm or inconvenience is most likely to result from improper access to sensitive member information because this type of information is most likely to be misused, as in the commission of identity theft.

Member Notice

Standard for Providing Notice

For purposes of the Guidance, sensitive member information means:

- A member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account.
- Sensitive member information also includes any combination of components of member information that would allow someone to log onto or access the member's account, such as user name and password or password and account number.

Member Notice

Standard for Providing Notice

- If a credit union, based upon its investigation, can determine from its logs or other data precisely which members' information has been improperly accessed, it may limit notification to those members.
- However, there may be situations where the credit union determines that a group of files has been accessed improperly, but is unable to identify which specific member's information has been accessed.
- If the circumstances of the unauthorized access lead the credit union to determine that misuse of the information is reasonably possible, it should notify all members in the group.

Content of Member Notice

- Member notice should be given in a clear and conspicuous manner.
- The notice should describe the incident in general terms and the type of member information that was the subject of unauthorized access or use.
- It also should generally describe what the credit union has done to protect the members' information from further unauthorized access.
- In addition, it should include a telephone number that members can call for further information and assistance.
- The notice also should remind members of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the credit union.

Content of Member Notice

The notice should include the following additional items, when appropriate:

- A recommendation that the member review account statements and immediately report any suspicious activity to the credit union;
- A description of fraud alerts and an explanation of how the member may place a fraud alert in the member's consumer reports to put the member's creditors on notice that the member may be a victim of fraud;
- A recommendation that the member periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;
- An explanation of how the member may obtain a credit report free of charge; and
- Information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft.
- The notice should encourage the member to report any incidents of identity theft to the FTC, and should provide the FTC's Web site address and toll-free telephone number that members may use to obtain the identity theft guidance and report suspected incidents of identity theft.

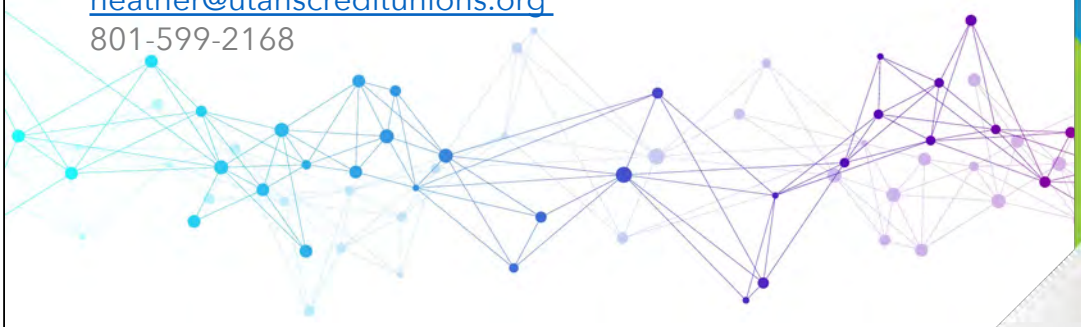
UTAH'S CREDIT UNIONS

Delivery of Member Notice

- Member notice should be delivered in any manner designed to ensure that a member can reasonably be expected to receive it.
- For example, the credit union may choose to contact all members affected by telephone or by mail, or by electronic mail for those members for whom it has a valid e-mail address and who have agreed to receive communications electronically.

Questions?

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



Coming Soon

Thursday April 11, 2024: Regulation CC, Twice (Rescheduled)