

## Identity Theft Checklist Supplement

- Provide member education through newsletter articles or statement stuffers, advising members to:
  - Review credit reports annually
  - Shred confidential documents
  - Review all account statements promptly
  - Use secure mailboxes to send and receive mail
  - Use caution when asked for personal information over the phone or Internet
  - Be aware of current scam tactics such as “phishing” and spoofing

Refer to sample brochures provided by the FTC and Credit Union National Association (CUNA). Links to these samples are provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html).

For more information on phishing scams, refer to <http://www.antiphishing.org> and NCUA Letter 04-CU-06 “E-Mail and Internet Related Fraudulent Schemes Guidance” (<http://www.ncua.gov/letters/2004/04-CU-06.pdf>).

- Provide employee training on ID theft.

Links to training provided by CUNA are provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html).

- Appoint a central contact person for members to deal with potential ID theft problems (as recommended by BITS).

Refer to the BITS white paper “Financial Identity Theft: Prevention and Consumer Assistance”. An Internet link to the white paper is provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html).

- Accept the Federal Trade Commission (FTC) “uniform affidavit” for members to report ID theft.

A link to affidavit is provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html). The affidavit is also included within the FTC brochure “When Bad Things Happen To Your Good Name”.

- Employees know and follow procedures on how to advise a member who is a victim of ID theft. At a minimum, the victim should be advised to:
  - Place fraud alerts with credit bureaus
  - Check credit reports

- Review accounts, use standard affidavit to report disputes
- Close accounts that have been tampered with or opened fraudulently
- File a police report (and keep a copy of the report for themselves)
- File a complaint with the FTC

Credit union employees should be familiar with these basic procedures. Fraud alerts provide notice to potential creditors that the person has been a potential victim of identity theft. The member only needs to notify one of the bureaus, which then notifies the other two credit bureaus. In addition, the member can place a victim statement on their credit profile, requesting creditors to contact the victim at a specific phone number prior to granting new credit.

After a victim places a fraud alert with the credit bureau, a free copy of their credit report will be sent to the victim by each credit bureau. The victim should review their credit reports for any signs of unauthorized activity.

One of the best resources to help victims through this process is the FTC brochure “When Bad Things Happen To Your Good Name”. Links to this brochure are provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html).

- Provide all ID theft victims a copy of the FTC brochure “When Bad Things Happen to Your Good Name”.

This is available from the FTC web site. The credit union can print a copy of the PDF file, or request a CD if they wish to have the brochure reprinted at a commercial printer. Internet links to this brochure are provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html).

- Credit union Web site contains a section on ID theft information, or contains a prominently placed link to an outside source of information.

Many credit union web sites devote a page to member education information on identity theft. At a minimum, a credit union site should refer members to a source of information, such as FTC’s consumer site: <http://www.consumer.gov/idtheft/>.

- Allow members to put a password on their accounts for inquiries or transactions.

The FTC recommends this to consumers within the brochure “When Bad Things Happen To Your Good Name”. You may want to notify existing members of this option, and expand your new account procedures to allow members to place passwords on their accounts.

- Have written procedures to provide security on telephone inquiries and guard against pretext calling that include one of the following: authorization codes, caller ID, or callback procedures.

These guidelines are provided by the NCUA in their letter 01-CU-09 “Identity Theft and Pretext Calling” (<http://www.ncua.gov/letters/2001/01-CU-09.pdf>).

- If you allow any funds transfer requests that are not in-person (by phone, fax or email), have written security procedures that require a callback.

UCC Article 4A ([http://www2.law.cornell.edu/cgi-bin/foliocgi.exe/ucc4a/query=\\*/doc/{t30}?](http://www2.law.cornell.edu/cgi-bin/foliocgi.exe/ucc4a/query=*/doc/{t30}?)) requires the use of commercially reasonable security procedures for fund transfers (this is also a requirement of most fidelity bond insurance contracts). This includes wire transfers, or transfers from one account at the credit union to another account at the credit union. Most credit unions meet this requirement through the use of a callback verification. A second option is the use of passwords assigned to the member, especially for employees of business members, which should be outlined in a written agreement with the member (following the provisions of UCC 4A).

Callback verification is an outgoing telephone call placed by you to verify the identity and authority of the sender of an instruction and which:

- a. You performed prior to executing the instruction; and
- b. You placed to a telephone number that you had independently determined to be valid for the authorized sender; and
- c. Resulted in confirmation that the instruction was sent by an individual you knew to be authorized to initiate such instruction.

Telephone identification procedures should prohibit staff from asking for member's name, account number, Social Security number, telephone number or mother's maiden name as a means of verifying the member's identity. Per UCC 4A, signature verification of a fax by itself, is not adequate; something additional like the callback procedure must also be done.

- If you offer an audio response system, the system uses a PIN that is not based on any portion of the member's Social Security Number.

PINs should not be based on "in wallet" or public directory information such as Social Security Numbers, birth date, telephone number, zip code, etc., nor be issued in a recognizable pattern (such as every member being issued the same PIN as the default). Refer to NCUA Letter 01-CU-10 "Authentication in an Electronic Banking Environment" (<http://www.ncua.gov/letters/2001/01-CU-10.pdf>) for more information.

- If you offer a home banking system, the system requires a password of at least 6 characters and avoids all use of any portion of member Social Security Numbers (including password resets or first-time activations).

Passwords should not be based on "in wallet" or public directory information such as Social Security Numbers, birth date, telephone number, zip code, etc., nor be issued in a recognizable pattern (such as every member being issued the same password as the default). Refer to NCUA Letter 01-CU-10 "Authentication in an Electronic Banking Environment" (<http://www.ncua.gov/letters/2001/01-CU-10.pdf>) for more information.

- Written address change procedures that require one of the following:
  - A confirmation mailed to both the old and new addresses, plus a minimum 30-day waiting period before sending any new/replacement plastic cards, PINs or checks.
  - A positive confirmation with the member (at a verifiable phone number) before sending any new/replacement plastic cards, PINs or checks within 30 days of the address change.

The address confirmation procedure is recommended by NCUA in their letter 01-CU-09 "Identity Theft and Pretext Calling" (<http://www.ncua.gov/letters/2001/01-CU-09.pdf>).

The positive confirmation is a requirement from the FACT Act ([http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108\\_cong\\_public\\_laws&docid=f:publ159.108.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf)), which requires new regulations to be adopted for this procedure. More information will be coming from the regulators this year.

- If you allow new member enrollment without a physical visit to a credit union location, use a third-party verification system (such as Primary Payment Systems® IDENTITY<sub>SM</sub> CHEK Web Service) to screen information supplied on new accounts. A third-party verification system is recommended for all new members.

The Patriot Act now requires customer identification procedures. A third party verification system is a good option for a non-documentary method of identification as mentioned in the Patriot Act. More information on the Patriot Act can be found in NCUA's Regulatory Alert 03-RA-07 "Final Patriot Act Regulations on Customer (Member) Identification" ([http://www.ncua.gov/reg\\_alerts/2003/03-RA-07.htm](http://www.ncua.gov/reg_alerts/2003/03-RA-07.htm)) and its enclosure ([http://www.ncua.gov/reg\\_alerts/2003/03-RA-07Encl.pdf](http://www.ncua.gov/reg_alerts/2003/03-RA-07Encl.pdf)).

More information on Primary Payment System's IDENTITY CHEK system is available at <http://www.primarypayments.com/>.

- Written or automatic procedures to identify potential ID theft on new loan applications. At minimum, the procedures should include verifying the address, date of birth, and employer information on the application, matching the information to what's found on the credit report, and resolving any discrepancies.

Refer to the BITS white paper "Financial Identity Theft: Prevention and Consumer Assistance". An Internet link to the white paper is provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html).

- Before you grant any new loans, you have a process to verify identity and comply with any fraud alerts the member may have on his or her credit bureau profile.

Refer to the BITS white paper "Financial Identity Theft: Prevention and Consumer Assistance". An Internet link to the white paper is provided in the online toolkits at [www.cunamutual.com/IDtheft](http://www.cunamutual.com/IDtheft) and [www.cuna.org/initiatives/idtheft.html](http://www.cuna.org/initiatives/idtheft.html).

- Registered to receive ongoing updates on education and ID theft issues through a trusted vehicle such as Credit Union National Association's *News Now*.

Individuals can sign up to receive News Now on the CUNA web site ([www.cuna.org](http://www.cuna.org)).

*This checklist was created by the CUNA Mutual Group and Credit Union National Association (CUNA) based on their experience in the credit union and insurance market. Neither CUNA Mutual nor CUNA provide any warranties or guarantees with respect to the checklist, which is intended solely as a guide, not as legal advice. No coverage is provided by this checklist.*