NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

DATE: May 2000 **LETTER NO.: 00-CU-02**

TO: All Credit Unions

SUBJ: Identity Theft Prevention

The purpose of this advisory is to bring to your attention the rising occurrence of identity theft in the financial marketplace. Identity theft occurs when someone hijacks a consumer's personal identifying information, such as their name, address, credit card or social security number, and uses the data to open new charge accounts, order merchandise, or borrow money. Many consumers have been victimized by identity theft already and the number of victims is rising exponentially. Congress addressed this concern with the passage of the Identity Theft and Assumption Deterrence Act of 1998. This act supplements existing laws that criminalize fraud by specifically addressing misappropriation of another's identity for criminal purposes.

The Federal Trade Commission (FTC), the Federal agency that investigates and concerns itself with such threats to consumers, is calling for increased private and public efforts to combat this crime. They have taken the lead in coordinating the efforts of government agencies and organizations to develop and disseminate comprehensive consumer education materials for victims of identity theft, and those concerned with preventing identity theft.

The National Credit Union Administration (NCUA) recently participated in an FTC sponsored National Summit on Identity Theft. I have enclosed information, from that event, on preventative measures that may help protect your members from identity theft. Please also be aware that if you suspect an illicit attempt to obtain information concerning a member's identity, you should report the matter to the appropriate authorities and file a Suspicious Activity Report (SAR). If you encounter victims of identity theft, refer them to the FTC Consumer Response Center at 1-877-FTC-HELP, for assistance in addressing their problems.

We encourage credit unions to proactively protect their members when dealing with information in commerce. Sensitivity to privacy and identity theft protection is a good business strategy.

Sincerely,

_____/s/_____
Norman E. D'Amours
Chairman
National Credit Union Administration Board

Enclosure

Enclosure

IDENTITY THEFT PREVENTION

Best Practices

These "best practice" suggestions offer guidance based on experience from actual identity theft. Not all of these suggestions will work for your credit union. Evaluate each suggestion and balance the privacy protection risk with the credit union's resources and products to develop privacy protection strategies and policies that are right for your credit union.

- Develop a comprehensive written privacy protection policy that includes responsible information handling practices. The privacy policy should address privacy and information handling for all the sensitive data held by the credit union, including data gathered from a website. The policy should cover all staff and officials of the credit union and their dealings with persons outside the credit union. It is beyond the scope of this Letter to provide comprehensive information on security and privacy strategies. However, we have appended some informational websites from experts in the field and encourage you to investigate further at libraries and technical bookstores.

- Display your credit union's Privacy Protection Policy in your literature and on your website.

- All staff, including credit union volunteers, should be trained on the credit union's security measures and privacy protection policies. Review and update the policies routinely and provide follow-up training. Even temporary and part-time employees, independent consultants, and vendors should have information on, and be subject to, the written policies.

- Conduct criminal and civil background checks before hiring employees who will have access to sensitive personal information. This includes screening services and temporary firms that the credit union uses, such as after hours cleaning companies.

- Limit the credit union's data collection to the information that is necessary for the stated purpose, and nothing more.

- Limit data disclosure. Restrict the addition of unnecessary data on printed documents. For example, social security numbers printed on documents such as pay or loan distribution checks, parking permits, staff badges, time sheets, mailing labels, account statements, etc.

- Prohibit using birth dates, social security, or driver's license numbers as account or personal identifier numbers.

- Restrict sensitive personal data to only those who have a legitimate need to know. Implement electronic audit trails and impose strict penalties for browsing and illegitimate access.

- Conduct better identity verification for instant credit, especially when an address is recently changed or is different from the credit report. Don't rely solely on social security numbers. Supplement with utility bills, tax records, etc.

- Train your staff to recognize and address incidents in which identify thieves use persuasive social engineering skills to obtain necessary pieces of information to enable them to complete identify theft.

- Put photographs on credit cards and staff business cards.

- Truncate digits on account numbers printed on transactions slips at point of sale terminals.

- Use account profiling systems to detect unusual activity. Notify members of potential fraudulent activity.

- Avoid mass mailing pre-approved offers of credit.

- Keep all information about employees locked in cabinets or encrypted data files. Establish data security procedures for those with legitimate access to the files.

- Encrypt sensitive personal and confidential information. Conduct "systems penetration tests" to determine if systems are "hacker proof."

- Ensure the credit union protects itself from "business identity theft, " such as mimic websites that entice your members to believe they are interacting online with the credit union.

- Adopt secure methods of disposing of sensitive personal information. Consider industrial shredders, locked garbage bins, etc. If disposal is outsourced, assure such companies have strict security procedures. Consider shredding software to delete confidential information from electronic data files.

- Train designated staff about security procedures in sending sensitive personal information via fax. Such faxes should have a confidential cover

letter (prohibiting re-disclosure), and the recipient should be called before sending, and called after, to confirm receipt.

- Prohibit the transmission of sensitive personal information by voicemail, cellular phones, pagers, answering machines, or e-mail, unless encrypted or sent via a secure network. None of these means of transmission is private or secure.

- Train customer service or fraud department staff how to work with identity theft victims. By helping the victim clear their record, you will limit your legal exposure to the victim.

- Don't share, sell, or transmit data about members without their permission. Guarding that information will limit your legal exposure if that information subjects your member to identity theft.

- Allow your members to inspect and correct their personal information. This practice will not only increase member's trust in your information handling practices, it will improve the accuracy of your files.

- Take every opportunity to become informed about financial fraud and identity theft. Join a local financial crimes group. Your local police or sheriff's department can inform you of such groups.

Relevant Publications

"Identity Theft: What to Do if it Happens to You" Available at: www.pirg.org.

"Identity Theft: When Bad Things Happen to Your Good Name" Available at: www.consumer.gov/idtheft.

Websites That Provide Further Guidance and Information

Federal Trade Commission - www.consumer.gov/idtheft and www.ftc.gov
U.S. PIRG and CALPIRG - www.pirg.org
Privacy Rights Clearing House – www.privacyrights.org
Identity Theft Survival Kit – www.identitytheft.org
Better Business Bureau – www.bbbonline.org