IDENTITY THEFT/FRAUD PREVENTION GUIDE & VICTIM CHECKLIST

Share this information with your family, friends and co-workers. If you become a victim of identity theft, please notify a Credit Union representative immediately.

PREVENTION

Keep Your Mail Safe

Criminals often steal mail in order to perpetrate fraud.

- Collect mail promptly from your mailbox.
- Ask the Post Office to hold your mail while you are away (i.e. vacation).
- Send all mail correspondence that contains personal and/or financial information from the Post Office or a secure, public mailbox.
- Many financial institutions offer the ability to opt out of paper statements for Estatements. Visit your Credit Union's website or local branch for additional details.

Stay Safe Online

There are several online threats such as phishing, malware, etc.

- Do not send sensitive information via email (i.e. credit card #).
- Make sure you are on a secure website when providing personal info online (the address contains https or shttp instead of http and the webpage often has a padlock icon).
- Avoid easy-to-figure-out passwords.
- Install firewall, anti-virus and spy ware protection on your computer. Keep them updated (especially if you use internet services from a public router)!
- Do not use a public computer when accessing your personal accounts or conducting financial transactions online.

Out of Site, Out of Mind

Fraud is often committed by the people you come in contact with on a daily basis.

- Avoid leaving personal info in "common areas" at home, work and/or school where teens, service/repair men, etc. can quickly access your records (e.g. kitchen counter, desk).
- Do not leave PINs or passwords in your wallet, on your desk or in other accessible areas-memorize them!
- Only carry the essentials in your wallet and/or purse.
- Shred or destroy unused financial solicitations, credit card applications and other financial documents (i.e. credit card/ATM receipts).

Know Your Audience

- Avoid giving personal information out in a public place. You never know who is listening.
- Do not give personal information over the phone including via text messages or computer unless you are sure of whom you are talking to and you initiated the contact.
- Reduce the amount of information you have printed on your checks (i.e. omit driver's license number, SSN). Remember individuals you write checks to and those who look over your shoulder while you are writing a check can easily memorize the information and use it to create counterfeit checks to commit fraud in your name.
- Beware of imposters! *Remember if it's too good to be true, then it probably is too good to be true.* Several websites identify and address the different types of scams.

Credit Cards

- Keep copies of your credit card account numbers and the phone numbers to report lost/stolen cards. Be sure to keep them locked up.
- Report lost/stolen cards immediately.
- Sign credit cards in permanent ink as soon as they are received.
- If you applied for credit, monitor the arrival of the new card. Contact the creditor immediately if you do not receive the new card within the anticipated time frame.
- If merchants use carbons for your credit card transactions, ask for the carbons so you can properly destroy them.

Proactive Steps

- Place a security freeze on your credit report. The security freeze prevents an identity thief from opening a new account or obtaining credit in your name. Each credit bureau has different requirements. Contact the Attorney General's Office www.iowaattorneygeneral.org/consumer/index.html for additional details. If you decide to apply for credit while the security freeze is active, you will need to plan ahead and contact the credit bureaus to temporarily release the security freeze.
- Deployed military personnel can place an active duty alert on their credit file.
- Protect your deceased relatives from identity thieves. Notify the Social Security Administration to add your deceased relative to the Death Master File. Be prepared to provide a copy of the death certificate. Contact the credit bureaus to place a "deceased" alert on his/her credit file. Contact any institutions where he/she had accounts and/or loans, as well as health insurers and the DMV.

Monitor

- Pay attention to your billing cycles and make sure you receive your financial statements on time. Notify the companies immediately if you have not received your statement in the appropriate time frame.
- Obtain a free credit report annually from each credit-reporting agency (877-322-8228 or www.annualcreditreport.com). It is recommended that you stagger them every 4 months so that your credit report is reviewed throughout the year rather than just once a year.
- Review your financial statements monthly and report any discrepancies immediately. A financial institution is not required to refund any monies if the discrepancy is not reported within the appropriate time frame. See the Rules and Regulations brochure or a Credit Union representative for the Credit Union's requirements.
- Monitor your credit report, SSN benefit statement, and/or medical insurer benefit forms regularly. Verify that there is not a criminal record in your name. Criminals do not always just use your personal info to commit financial fraud. They may also commit crimes, apply for jobs and/or receive medical benefits in your name.

IDENTITY THEFT VICTIM CHECKLIST

This checklist is a guide to help you recover from identity theft and to prevent future fraud in your name and on your accounts.

TAKE ACTION IMMEDIATELY!

- File a police report with local authorities. Obtain a copy of the report for your records.
- Contact **one** of the three major credit bureau's fraud departments to place an initial fraud alert on your account. The credit bureau you contact is then responsible for contacting the other two bureaus. The initial fraud alert remains on your credit report for at least 90 days and entitles you to a free credit report from each of the three credit reporting agencies. You can also place an extended fraud alert on each of your credit reports. The extended alert remains on your account for 7 years, entitles you to 2 free credit reports from each credit reporting agency within 12 months and removes your name from marketing lists. The extended fraud alert requires an official ID theft report.

Equifax	**Experian**	**TransUnion**
P.O. Box 105069,	PO Box 2104	PO Box 1000
Atlanta, GA	30374 Allen, TX 75013-2104	Chester, PA 19022
(800) 685-1111	(888) 524-3606	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com

- Complete and sign a Forgery Affidavit (if Credit Union accounts were compromised).
- Close all compromised accounts at all financial institutions.
- Complete the ID Theft Affidavit (located in "Take Charge: Fighting Back Against Identity Theft" at www.ftc.gov/ Provide this affidavit anywhere a **new** account was opened in your name.
- File complaint with Federal Trade Commission www.ftc.gov/

IMPORTANT NOTES

Keep a log of all conversations (name, date and time) when dealing with financial institutions and legal authorities.

- Always follow up phone calls with a letter that outlines your phone conversation.
- Send all correspondence by certified mail requesting receipt.
- Keep copies of all correspondence and establish a filing system to organize them.
- Keep old files even if you believe your case is closed should problems arise in the future.

OTHER ADVISABLE STEPS/CONSIDERATIONS

When considering these steps, do not forget minors and elders. They are often the victims of identity theft.

- Opt out of paper statements from the Credit Union. You will still be able to view your statements online. Ask a Credit Union representative for additional details.
- Place a security freeze on your credit report. The security freeze prevents an identity thief from opening a new account or obtaining credit in your name. Each credit bureau has different requirements. Contact the Attorney General's Office at www.iowaattorneygeneral.org/consumer/index.html
- Contact Social Security Administration at (800) 772-1213 to verify the accuracy of the earnings reported to your SSN, to request a replacement card or a copy of your Social Security statement.
- Notify the DMV if your driver's license number was used to obtain fraudulent credit. You can request a new driver's license number.
- Notify the US Postal Inspection Service or go to www.usps.gov if you suspect mail theft or fraud.
- Contact check verification companies to have them notify their respective clients (retailers) not to accept or authorize your checks on your compromised account(s).
- Notify Passport Authorities if your passport was stolen, missing or used fraudulently.
- Notify utility companies if services have been established in your name.
- Review benefit forms from medical insurer for accuracy and notify the insurer immediately if you discover any errors.
- Review criminal records to ensure crimes have not been committed in your name. Contact your county's Clerk of Court office for additional information.
- Continue to monitor your credit reports and financial account statements and report any irregularities immediately.