IDENTITY THEFT/FRAUD PREVENTION GUIDE

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. 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. For additional information, please visit your Credit Union's website.

- 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. Passwords should be at least eight characters long, preferably using letters, numbers, and/or symbols.
- Carry PINs and passwords in your head and do not put them in your wallet or purse.
- 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.
- Make sure your home wireless router is encrypted and password protected.
- When selling items online, watch out for (real looking) fake checks and money orders. Be wary of overpayments or endorsed checks. Never wire "excess" payments back to the buyer or someone else.

Out of Sight, 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).
- Shred or erase hard drives from copiers, printers, and computers that may hold confidential information.

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.

Credit Cards/Rewards 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.
- Remove grocery or department store rewards cards from your key chain. If possible, remove name and/or address from these cards as well. It is possible for a person to find/steal a set of keys, scan the rewards tag on the key chain to determine the key's owner and possibly their home address, and use this information to break into their home.

Proactive Steps

- The NC Attorney General's Office recommends that you 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.ncdoj.com or call (877) 566-7226 (toll free within NC) 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.
- Opt out of prescreened credit offers at 1-888-5-OPT-OUT or www.optoutprescreen.com
- 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 at (800) 772-1213 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.