Identity Theft

IDENTITY THEFT IS FRAUD COMMITTED OR ATTEMPTED USING THE IDENTIFYING INFORMATION OF ANOTHER PERSON WITHOUT THEIR AUTHORITY.

IDENTITY THEFT METHODS

- **Dumpster diving:** Rummaging through trash to look for bills and other documents containing personal information.
- **Skimmers:** Electronic storage devices that steal credit or debit card information from a card's magnetic strip. These are commonly found attached to ATMs, fuel pumps, and point-of-sale machines at restaurants and retail stores.
- **Phishing, Smishing, or Vishing:** Sending spam through e-mail or pop-up messages online, text messages, or voicemail messages to trick you into revealing personal information.
- **Address change:** Diverting your statements or other mail to another location where thieves have access.
- **Stealing:** Stealing wallets and purses, preapproved credit offers, new checks, tax information, etc.
- **Pretexting:** Obtaining your information under false pretenses.
- **Synthetic ID theft:** Combining a Social Security number with an unrelated name and birth date.

WHAT DO IDENTITY THIEVES DO WITH A STOLEN IDENTITY?

- **Credit fraud:** Open new credit accounts or run up charges on existing lines of credit.
- **Utilities fraud:** Use stolen information to open phone, power, gas, or cable accounts.
- **Financial fraud:** Open new accounts, take over existing accounts, or apply for loans.
- **Government documents fraud:** Use stolen information to obtain a driver's license, file a tax return, or obtain government benefits.
- **Other fraud:** Use stolen information to rent an apartment, obtain medical services, provide false information to police during an arrest, etc.

HOW TO DETERMINE IF YOU ARE A VICTIM OF IDENTITY THEFT*

- Monitor your accounts for unexplained charges or withdrawals.
- Check your credit report annually.
- Take note and take action if you:
  - Do not receive expected bills or other mail (the thief may have changed your address).
  - Receive credit cards for which you did not apply.
  - Are contacted by companies about merchandise or services you did not purchase.

*Adapted from the Federal Trade Commission's "Taking Charge: What to Do If Your Identity Is Stolen."

WHAT TO DO IF YOUR IDENTITY IS STOLEN

If you think your identity has been stolen, follow these instructions immediately:

1. File a police report.
2. Close the accounts you think have been compromised or opened fraudulently.
3. Contact one of the following credit reporting agencies to place a fraud alert on your credit reports. (Each agency is required to notify the other two agencies.)
   - Equifax | (800) 525-6285 | www.equifax.com
   - Experian | (888) 397-3742 | www.experian.com
   - TransUnion | (800) 680-7289 | www.transunion.com
4. File a complaint with the Federal Trade Commission (FTC):
   - Online: www.identitytheft.gov
   - By Phone: (877) 438-4338

For more information, visit the FTC's website at www.consumer.ftc.gov.

At SECU, we're dedicated to ensuring you have the tools and resources you need to meet your goals. Visit your local branch Monday through Friday, 8:30 a.m. to 5:30 p.m., or call our Member Services Support at (888) 732-8562.

SECU
State Employees' Credit Union®