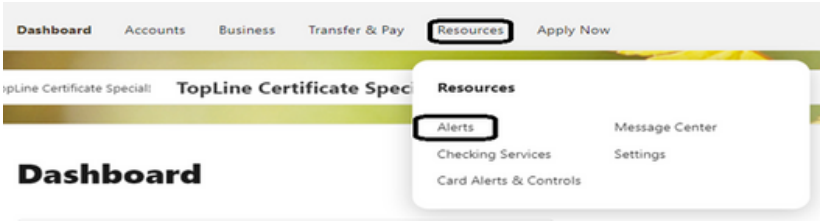
TOPLINE'S DO'S AND DON'TS TO PREVENT FRAUD

DO'S

- Do keep an eye on your online banking. You can set up alerts for many things, such as changes to your personal information, deposits and withdrawals. These customizable alerts can be found under the Resource Tab in your Online Banking.



- Do check out our Fraud Prevention tools on our website. These can be found by going to Toplinecu.com, Resources Tab, and Fraud Prevention.
- Do reach out to TopLine if you feel your information has been compromised. We will walk you through the next steps that need to be taken
- Do ensure that your contact information is up to date at all of your financial institutions. This way you can be reached if there is suspicious activity on your accounts.
- Do be wary of the websites you are putting your card/account information into. Always research a website you are shopping on to make sure they are legitimate, as some websites can be fraudulent
- Do use strong passwords. Use a mix of numbers, letters and special characters to make it harder for hackers to figure out
- Do freeze your credit if you feel your personal information has been compromised. Freezing credit will prevent new lines of credit being opened using your information. The three credit bureaus to contact are:
  - Equifax: 800-685-1111
  - Experian: 888-397-3742
  - Transunion: 888-909-8872

DON'TS

- Don't give out personal information over the phone if you are unsure of who you are speaking to. TopLine will NEVER contact you and request personal information. If someone contacts you requesting information, hang up and call TopLine at 763-391-9494 and we can assist you further
- Don't give out your PIN, Card Number, Account Numbers, or Verification Codes (MFA Codes) to someone requesting them via phone, email, or mail. If someone is attempting to obtain this information from you, please reach out to TopLine for further assistance
- Don't transfer money at the request of someone else. Please reach out to TopLine if someone is asking you to do this
- Don't respond to any unsolicited phone calls, texts, or emails that ask for information
- Don't download apps on your phone or computer at the request of someone you do not know
- Don't leave passwords easily accessible, such as sticky notes near your computer, or writing your PIN on your debit card. Easily accessible passwords could lead to your information being compromised
- Don't use the same password for multiple websites/accounts
- Don't use personal information in your password (birth year, address, last name, etc.)