

CONFIDENTIALITY AND SECURITY

We restrict access to nonpublic information about you to those employees who need to know that information to provide products or services to you. We maintain physical, electronic and procedural safeguards that comply with federal standards to guard your nonpublic personal information. If you ever have questions or concerns about the integrity of your account information, please contact us.

TO CONTACT US:

E-Mail: info@affiliatedtradescu.org
Phone: 610-489-0161
Fax: 610-489-2690
Mail: 3900 Ridge Pike, Collegeville, PA 19426

IDENTITY THEFT

Protect yourself from the potential of identity theft. Federal agencies recommend these steps to help yourself from this growing problem

- Review credit reports annually.
- Shred confidential documents.
- Review account statements promptly
- Use a secure mailbox to send and receive mail.
- Use caution when asked for personal information over the phone or internet.
- Be aware of current scam tactics such as “phishing and spoofing”.

If you believe you may be the victim of identity theft:

- Contact the Federal Trade Commission (FTC) and file a complaint
- Place a Fraud Alert with a National Credit Reporting Agency
 - Transunion 800-680-7289
 - Experian 888-397-3742
 - Equifax 888-766-0008
- Check your Financial Accounts
- Check your Computer for Viruses
- Secure your Proof of Identity
- File a Police Report
- Keep a Record of your Actions
- Order Credit Reports for Review
- Don't Ignore the Activity

BEST PRACTICES FOR ONLINE SECURITY

- Use strong, complex passwords that contain:
 - alpha/numeric characters and symbols
 - upper and lower case characters
 - minimum of 8 characters but longer is recommended
 - no real words or names of family/friends/ pets
 - use entire keyboard; avoid strings of identical characters
- Change your passwords regularly and use a different password for each website you access.
- Never reveal your confidential login ID, password, PIN or answers to security questions to anyone.
- Never bank online using computers at kiosks, cafes, unsecured computers or unsecured wireless networks.
- Prohibit the use of shared user names and passwords for your online banking accounts.