Keeping Your Accounts Secure

We recognize the importance of safeguarding your financial accounts and your personal information against the ongoing risk of fraud, cyber threats, and other unauthorized activity. This is essential to building a successful partnership and maintaining your trust. You play an important role and are the first line of defense when it comes to protecting your accounts and identity.

We believe that keeping your account secure is a mutual responsibility, therefore we highly recommended taking the following key steps.

1. Register your account online.
2. Review your account information on a regular basis and keep your contact information current.
3. Promptly report any suspected identity theft or unauthorized activity.
4. Practice safe computing habits.

ADDITIONAL TIPS ON KEEPING YOUR ACCOUNT SAFE AND SECURE

GENERAL PASSWORD SECURITY

- Use a unique 6-12 characters alphanumeric username and password for each site where you maintain an account and regularly update your passwords. Never use your date of birth or Social Security number as your password.
- Setup multi-factor authentication with a mobile phone number.
- Don't allow social networking sites to memorize your passwords.
- Don't share your password or answers to security questions with anyone. In general, your account numbers, PINs, passwords and personal information are the keys to your accounts.
- The strongest passwords are comprised of a chain of unrelated common words.

BEWARE OF FRAUDULENT EMAILS OR PHISHING

- Be suspicious of emails asking for your confidential information and never provide credentials.
- Look out for red flags such as urgent requests, unknown email addresses or discrepancies between actual and displayed hyperlinks.
- Be aware that fraudulent emails can appear to come from a business that you are working with. Always review sender name, email, and web address to ensure they are from legitimate sources.
- We will never ask you for your personal information by email.

TAKE CARE OF YOUR COMPUTER AND MOBILE DEVICES

- Update your computer by installing the latest software and patches to prevent hackers or viruses from exploiting any known weaknesses.
- Install and update anti-virus software to protect your computer and to prevent hackers from installing malware or viruses on your computer.
- Check your operating system to see if firewalls are included. If not, be sure to install a firewall to regulate the flow of information between computers.
- Use only programs from a known, trusted source.
- Backup your important files on a regular basis and store the backups in a secure place.

HOW WE KEEP YOUR ACCOUNTS SAFE

- We have strict privacy and security policies. Protecting participant data is our number one priority, we safeguard account data with strong encryption, firewalls, and secure email.
- We employ sophisticated technologies and best practices to make sure your sensitive information and accounts are well protected online and over the phone. We utilize Multi Factor Authentication (MFA) and third-party security question routines to confirm your identity.
- We utilize proactive 24/7 system surveillance, if suspicious activity is detected, our security team receives alerts to investigate.
- We vigilantly monitor all our physical locations to prevent theft or unauthorized use of your sensitive information. In addition, authorized personnel can only enter work areas through use of a security badge.

WHAT TO DO IF YOU ARE A VICTIM OF A DATA BREACH

- Consider changing any PIN or password used to access your financial accounts, especially if the PIN or password contains any part of your Social Security number or date of birth.
- Sign up for account alerts or electronic delivery of notices from your financial institutions if available.
- Order copies of your credit reports from the three national credit-reporting agencies. Then, look for accuracy or indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries, defaults and delinquencies that you did not cause.

WHAT TO DO IF YOUR IDENTITY HAS BEEN STOLEN

Visit the federal government's website www.identitytheft.gov for detailed instructions on how to report and recover from identity theft. This site provides streamlined checklists and sample letters to guide identity theft victims through the recovery process.

- Contact us, your employer, and other financial institutions and credit card issuer(s) to inform them that your identity has been stolen.

24-085 (8/25)