KLINGENSTEIN FIELDS
ADVISORS

Preventing Fraud

Steps to safeguard your assets

QUICK STEPS TO HELP YOU

1 Fortify your online security

2 Support safekeeping of your personal information

3 Protect your money

USE STRONG PASSWORDS

- Don't allow browsers to save or store passwords.
- Create unique passwords for financial institutions and change frequently. Use 8-12 characters with a combination of cases, symbols, and numbers.
- Consider a password manager to store and manage passwords.
- Use two-factor authentication when possible, through hard or soft tokens.
- Keep your passwords confidential and secured.

SURF SAFELY

- Only use wireless networks that are protected.
- Look for websites that start with https vs. http.
- Pay attention to pop-up security warnings.
- Don't accept software updates when connected to public Wi-Fi.
- Consider a virtual private network (VPN) to enable network access in public locations or use a Wi-Fi hot spot.

PROTECT YOUR ASSETS

- Consider using VoiceID or a verbal password for your phone interactions with client service centers.
- Frequently review your financial and phone statements.
- Perform due diligence when sending funds to a third party and be on the lookout for possible scams:
  - Contact the recipient by phone and ask for supporting documentation.
  - For goods, you should view the merchandise before agreeing to purchase.
  - Perform online searches, check with the BBB, and conduct other due diligence in confirming the legitimacy of the offer. Understand the details of the request.
  - Verify that communications purporting to be either from or on behalf of individuals you know are valid.
- Use caution when deciding who to share personal information with via phone or email.
- Change passwords periodically, especially when prompted to do so by an online account provider.

LIMIT INFORMATION YOU SHARE ONLINE

- Use good judgment when choosing what to share on social media. Information can be pulled from profiles and used to perpetrate ID theft.
- Set privacy/security settings on your social media profiles.

USE SAFE EMAIL PRACTICES

- Do not click on links or attachments included in emails and texts as they could be a phishing attempt.
- Hover over links or requests to click to see the true URL and confirm if legitimate.
- Leverage a spam filter.
- Do not enter your username and password into a website that was received by an email. Go directly to the trusted website where the account is held to login.
- Email communications containing personal information should be encrypted, if possible.
- Be on the lookout for "email spoofing," where an email appears to be from a person or business that you know, but it is actually a scam. If you are unsure, contact the supposed sender directly.

EMPLOY EQUIPMENT SAFETY

- Keep your web browser and operating system updated and activate the firewall.
- Install antivirus and antispyware software on all platforms and run scans on a regular basis.
- Check security settings on your applications and web browser, and make sure they're strong.
- Use a passcode or thumbprint to secure mobile devices.
- Do not use or access disks, flash drives or other removable media that are left in open/public areas as they could contain viruses.
- Use caution when allowing your computer or device to store and autofill passwords, especially if others have access to your computer or device.

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."

— Newton Lee, *Counterterrorism and Cybersecurity: Total Information Awareness*

INDUSTRY RESOURCES

- Go to StaySafeOnline.org and review the STOP. THINK. CONNECT.™ cybersecurity educational campaign
- Visit OnGuardOnline.gov, also a part of the STOP. THINK. CONNECT.™ campaign, that focuses on online security for kids and includes a blog on current cyber trends
- Visit fbi.gov/scams-safety/fraud to learn more about common fraud schemes

KLINGENSTEIN FIELDS
ADVISORS

125 Park Ave Suite 1700 New York, NY 10017 (212) 492-7000 klingenstein.com