08.03.21 | FIRM ANNOUNCEMENTS

Cybersecurity & Fraud Prevention

Michael Davide – Chief Compliance Officer, Controller

Keeping your information secure from criminals is a top priority for our firm. To better protect you and your accounts from cybersecurity threats, we continuously review security procedures to ensure that we are following best practices recommended by the custodians, financial institutions, and industry experts with whom we work.

While we feel we are taking clear and actionable steps in our own firm's security measures, cyber fraud continues to escalate, is becoming more sophisticated, and is ever-changing. The threats take various forms. For example, email scams (such as phishing), where criminals obtain investors' identities and use that information to commit various forms of wire fraud. Cybercrime and fraud are serious threats and constant vigilance is key. While Grimes & Company plays an important role in helping protect your assets, you can also take action to protect yourself and secure your information.

The list below summarizes common cyber fraud tactics, along with tips and best practices for keeping your information safe. Many suggestions may be things you are doing now, while others may be new. We also cover actions to take if you suspect that your personal information has been compromised. If you have questions, we are here to help. Here are some ways we can work together to protect your information and assets:

SAFE PRACTICES FOR COMMUNICATING WITH OUR FIRM:

- **Keep us informed** regarding changes to your personal information.
- **Expect us to call you to confirm email requests** to move money, trade, or change account information.
- **When sending confidential information,** utilize our secure email service or securely upload via our website.
- Feel free to contact our office to verify authenticity of any Custodian (Fidelity, TD Ameritrade or Charles Schwab) emails.

WHAT YOU CAN DO:

- Be aware of suspicious phone calls, emails, and texts asking you to send money or disclose personal information. If a service rep calls you, hang up and call back using a known phone number.
- Never share sensitive information or conduct business via email, as accounts are often compromised.
- Beware of phishing or malicious links. Urgent-sounding, legitimate-looking emails are intended to tempt you to accidentally disclose personal information or install malware.
- Do not open links or attachments from unknown sources. Enter the web address in your browser.
- Check your email and account statements regularly for suspicious activity.
- Never enter confidential information in public areas. Assume someone is always watching.

EXERCISE CAUTION WHEN MOVING MONEY:

- Review and verbally confirm all disbursement request details thoroughly before providing your approval, especially when sending funds to another country. Never trust wire instructions received via email.

MAINTAIN UPDATED TECHNOLOGY:

- Keep your web browser, operating system, antivirus, and anti-spyware updated and activate the firewall.
- Do not use free/found USB devices. They may be infected with malware.
- Check security settings on your applications and web browser. Make sure they are strong.
- Turn off Bluetooth when it is not needed.
- Dispose of old hardware by performing a factory reset or removing and destroying all data storage devices.

USE CAUTION ON WEBSITES AND SOCIAL MEDIA:

- Do not visit websites you do not know (e.g., advertised on pop-up ad banners).
- Log out completely to terminate access when exiting all websites.
- Do not use public computers or free Wi-Fi. Use a personal Wi-Fi hotspot or a Virtual Private Network (VPN).
- Hover over questionable links to reveal the URL before clicking. Secure websites start with “https”, not “http”.
- Be cautious when accepting “friend” requests on social media, liking posts, or following links.
- Limit sharing information on social media sites. Assume fraudsters can see everything, even if you have safeguards.
- Consider what you are disclosing before sharing or posting your résumé.

WHAT TO DO IF YOU EXPECT A BREACH:

- Call our office immediately so we can watch for suspicious activity and help with necessary steps to protect your investment accounts. TD Ameritrade, Fidelity and Charles Schwab have online fraud policies in place that pledge to reimburse assets stolen due to unauthorized online transactions. They can also restrict your accounts or change your account numbers to prevent fraudulent distributions.
- Change your passwords for all services, including email, financial sites, social networking sites, etc.
- If you are the victim of tax fraud, visit the IRS website to access the "Taxpayer Guide to Identity Theft", which provides education on tax-related identity theft, tips to reduce your risk, and steps for victims to take.
- If you suspect your social security number has been compromised, contact the Social Security Administration's fraud hotline at 800-269-0271. The Office of the Inspector General will take your report and investigate activity using your Social Security Number. The Social Security Administration also provides helpful materials, such as the pamphlet "Identity Theft and Your Social Security Number".
- Consider placing a fraud alert or credit freeze with Experian, TransUnion or Equifax.

LEARN MORE:

- **StaySafeOnline.org:** Review the STOP. THINK. CONNECT™ cybersecurity educational campaign.
- **OnGuardOnline.gov:** Focused on online security for kids, it includes a blog on current cyber trends.
- **FDIC Consumer Assistance & Information**
- **FBI Scams and Safety provides additional tips**

Do not hesitate to contact us with questions or concerns about how we protect your accounts or the steps you and your family can take to better protect yourselves and mitigate risk. As always, we appreciate the opportunity to help you achieve your financial goals.

A copy of the Grimes' current written disclosure Brochure discussing our advisory services and fees continues to remain available upon request or at www.grimesco.com. **Please Remember:** If you are a Grimes client, please contact Grimes, in writing, if there are any changes in your personal/financial situation or investment objectives for the purpose of reviewing/evaluating/revising our previous recommendations and/or services, or if you would like to impose, add, or to modify any reasonable restrictions to our investment advisory services. Unless, and until, you notify us, in writing, to the contrary, we shall continue to provide services as we do currently. **Please Also Remember to advise us** if you have not been receiving account statements (at least quarterly) from the account custodian.