SFM
STACK FINANCIAL MANAGEMENT

(406) 862-8000
sfm@StackFinancialManagement.com

Safety First: In Your Portfolio and Beyond

An increasingly digital financial landscape requires that we balance the efficiencies which technology offers with the need to guard against cybersecurity threats.

Our team prioritizes your security and recognizes the importance of partnering with you in a commitment to safety. The purpose of this communication is to keep you informed of cybersecurity issues and empower you to participate in the digital world in ways that maximize convenience while mitigating risk.

How Does SFM Protect You?

- **Client Authentication Procedures** – The Stack Financial Management (SFM) team follows strict protocols to verify client identity prior to processing a transaction or account change. This process is not intended to make it difficult for you to access your account(s), but to prevent a fraudster from accessing your account(s).
- **Cybersecurity Measures** – We follow the best practices outlined in Charles Schwab & Co's (Schwab) Cybersecurity Resource Program, including the use of multi-factor authentication for access to online client data.
- **Staff Training** – Our team meets regularly to discuss best practices and common pitfalls, including phishing scams and money movement fraud. We also participate in training conducted by Schwab's cybersecurity and fraud experts.
- **Vendor Assessment** – We routinely take steps to research our new and existing vendors and ensure that their security protocols are up-to-date.

How Does Schwab Protect You?

- **Cutting-Edge Tools and Technology** – Schwab's software can recognize unusual account activity that can assist in the prevention of fraudulent account transactions.
- **Multi-factor Authentication** – Schwab uses multi-factor authentication (MFA) to ensure that unauthorized parties are not able to access your accounts.
    - When you log in to your Schwab account, a strong password will be required. Your digital access will be locked out after too many invalid login attempts.
    - When you call Schwab, they will authenticate your identity before processing any account transactions.
- **Company Culture and Commitment** – Schwab's employees are required to complete ongoing security training, and Schwab continually reinforces data protection importance in various ways.
    - Schwab provides cybersecurity education to employees and clients alike.
    - View their Fraud and Security Video Library here.

How Can You Protect Yourself?

- **Prioritize Email and Text Security** – Protect yourself from phishing attempts.
  - Do not click on links or attachments if you have a suspicion about the validity of the sender. Phishing scams are becoming more sophisticated and will often look like a legitimate email or text from your bank, credit card company, or another known contact.
  - If the email address associated with your SFM account(s) has been compromised, contact our office as soon as possible.
- **Surf Safely** – Don't conduct business on public Wi-Fi networks, and instead consider using a personal hotspot or virtual private network (VPN).
  - Log out of sites completely when you are done to terminate access.
  - Don't visit unknown websites advertised by pop-ups and banners.
- **Share Information Sparingly** – Be cautious about the information you share on social media sites and in phone conversations with unknown parties.
  - Be cautious when accepting "friend" requests and opening direct messages.
- **Use Strong Credentials** – Create unique, strong passwords for each website and don't share login credentials.
  - Don't use personal information as part of your password.
  - Change passwords regularly, at least every 6 months.
- **Monitor Account Activity** – Regularly check account statements for unusual or unexpected activity.
- **Check Your Computer for Malware** – Periodically perform a full anti-virus and anti-spyware scan on your computer and other devices.

How Can You Get Help?

- **Don't Hesitate** – If you suspect that you have been the victim of fraud or a data breach, don't be afraid to ask for help. Falling victim to a fraudulent scheme is not a reflection of you; it reflects the increasing sophistication with which fraudsters operate.
  - Reach out to the SFM team as soon as possible. Contact us via phone at 406-862-8000.
  - Contact the Schwab Identity Theft line at 877-862-6352.
  - Consider involving a trusted family member or friend. Fraudsters benefit when you feel isolated and overwhelmed, and support from a loved one can help you navigate the situation.
- **Take Inventory** – Refer to the Schwab Identity Theft Checklist for clear and detailed next steps. This checklist covers reporting procedures, system security measures, and additional monitoring recommendations.

Our mission is for you to sleep soundly at night knowing that your assets, information, and identity are secure. If you have any questions or concerns about the security of your SFM account(s), please reach out to us at 406-862-8000.