charles SCHWAB

Instructions for using the **Tips for Preventing Fraud** client checklist

With minimal risk and the potential for significant rewards for fraudsters, cybercrimes and fraud are a constant threat. You have a strong cybersecurity plan and have fostered a culture of vigilance among your employees, but your clients are targets, too. Fortunately, they can proactively take steps to help reduce their risk. This checklist, which you can customize and share with your clients, contains tips and best practices to protect their data, information and assets, and help prevent fraud. It also suggests what to do if they suspect their information or accounts may have been compromised.

Customization

You can customize this checklist prior to sharing it with clients. For example, you can add or edit information. To include your firm's name and/or logo, select and delete the YOUR LOGO Your Firm Name image, and copy and paste your logo or type in your firm's name. If you choose to keep the "What to do if you suspect a breach" section, consider customizing our "How to Respond to a Data Breach" flyer and saving your version so that it can easily be shared with your clients.

Resources

Schwab verified the resources and websites referenced in this document in October 2020. Websites and phone numbers may change. To ensure accuracy, we recommend that you verify all these resources and become familiar with them prior to sharing the handout with your clients.

Own your tomorrow®

Tips for preventing fraud

Cybercrime and fraud are serious threats and constant vigilance is key. While my firm plays an important role in helping protect your assets, you can also take action to protect yourself and help secure your information. This checklist summarizes common cyber fraud tactics, along with tips and best practices. Many suggestions may be things you're 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're here to help.

Cyber criminals exploit our increasing reliance on technology. Methods used to compromise a victim's identity or login credentials – such as malware, phishing, and social engineering – are increasingly sophisticated and difficult to spot. A fraudster's goal is to obtain information to access to your account and assets or sell your information for this purpose. Fortunately, criminals often take the path of least resistance. Following best practices and applying caution when sharing information or executing transactions makes a big difference.

How 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.
- **Establish a verbal password** with our firm to confirm your identity or request a video chat.

How Schwab protects your account

Schwab takes your security seriously and leverages protocols and policies to help protect your financial assets. Below are actions you can take to reinforce their efforts and resources to assist you in keeping your account safe:

- **Confirm your identity** using Schwab's voice ID service when calling the Schwab Alliance team for support.
- **Use two-factor authentication**, which requires you to enter a unique code each time you access your Schwab accounts.
- **Review the Schwab Security Guarantee**, which will cover losses in any of your Schwab accounts due to unauthorized activity. To learn more, visit Schwab's Client Learning Center.

Follow general best practices

- **Be suspicious** of unexpected or unsolicited phone calls, emails, and texts asking you to send money or disclose personal information. If you receive a suspicious call, do not accept it, hang up, and call back using a known contact number.
- **Be cautious when sharing sensitive information** and conducting personal or confidential business via email, since it can be compromised and used to facilitate identity theft.
- **Do not disclose personal or sensitive information on social media sites**, such as your birthdate, contact information, and mother's maiden name.
- B**e cautious when receiving money movement instructions via email**. Call the sender at their known number (not a number provided in the email) to validate all instruction details verbally before following instructions or providing your approval.
- Protect yourself from phishing attempts and malicious links (see glossary for additional information).

- Check your email and account statements regularly for suspicious activity.
- **Do not verbally disclose or enter confidential information** on a laptop or mobile device in public areas where someone could potentially see, hear, or access your information.
- **Verify payment requests you receive by phone or email**. Requests for you to make payments using prepaid debit cards, gift cards, or digital currency are frequently associated with fraud or scams.

Keep your technology up to date

- **Keep your web browser and operating system up to date**, and be sure you're using appropriate security settings. Old software, operating systems, and browsers can be susceptible to attack.
- **Install anti-virus and anti-spyware software** on all computers and mobile devices.
- **Enable the security settings** on your applications and web browser.
- **Do not use free or found USB thumb drives**—they could be infected with viruses or malware.
- **Turn off Bluetooth** when it's not needed, to protect against individuals gaining access to your devices using Bluetooth connections.
- **Safely and securely dispose of old hardware.**

Be cautious with public networks

- **Avoid using public computers.** If you must use one, go to the browser settings and clear the browser history (cache) and cookies when you're finished.
- **Only use wireless networks you trust** or that are protected with a secure password.
- **Use your personal Wi-Fi hotspot** instead of public Wi-Fi.
- **Do not accept software updates** if you are connected to public Wi-Fi.

Be strategic with your login credentials and passwords

- **Do not use personal information** such as your Social Security number or birthday as part of your login ID.
- **Create a unique password** for each financial institution you do business that are long and contain a combination of characters, numbers, and symbols. Consider using a password manager to create, manage, and store passwords that are unique and secure.
- **Do not share your passwords.**
- **Use two-step verification whenever possible.**

Be sure you're on a secure website

- **Check the URL to see if it's a secure connection.** Secure sites begin with https rather than http, and are generally considered safer.
- **Check the address bar for site validity** indicators whenever you log in to a Schwab website. Some browsers use green text or security symbols to indicate a secure and verified site.
- **Download apps only from the Google Play™ Store or the Apple App Store®.**
- **Do not visit websites you don't know**—for example, websites advertised on pop-up ads and banners.
- **Log out completely** to terminate access when you've completed a secure session, such as with online banking or a credit card payment.

Beware of phishing

- **Do not click on links or attachments** in emails and text messages if you question the validity of the sender. Instead, type the real web address, for example https://www.schwabalIiance.com, in your browser.
- **Hover over questionable links** to reveal the site's full URL and see where the link really goes. Do not click on links that don't match the sender or don't match what you expect to see.
- **Be suspicious** of emails that have grayed-out Cc: and To: lines—they may have been sent to a mass distribution list.
- **Check the sender's domain name in the email address** (john.doe@schwab.com) to see if it matches what you would expect to see.
- **Activate the spam filters** in your email settings tab. This will help prevent unsolicited emails from coming to your inbox.
- If you suspect an email that appears to be from Schwab is a phishing email, forward it to phishing@schwab.com.
- **If you have questions about an email from Schwab** or personal information you entered about your Schwab account after clicking an email link, call your advisor or the Schwab Alliance team immediately at **800-515-2157**.

What to do if you suspect a breach

- Call my office or your Schwab Alliance team immediately at **800-515-2157** so that they can watch for suspicious activity and collaborate with you on other steps to take.
- Request Schwab's "How to Respond to a Data Breach" flyer for more information.

Glossary

Two-step verification (aka multi-factor authentication)

A method of confirming your identity using a second step to verify who you are. For example, the first step might be to enter your username and password, and the second step might be to enter a randomly generated number sent to you via email, text, phone call, or token.

Phishing

The fraudulent practice of sending emails or text messages appearing to be from reputable companies or trusted individuals in an attempt to get individuals to reveal personal information such as passwords and credit card numbers. Phishing attempts are usually urgent-sounding, legitimate looking emails or texts designed to trick you into disclosing personal information or installing a virus on your device. These scams can be sent as attachments or links that, when opened or clicked, may trigger malicious activity or take you to fake sites that resemble the real business websites.

Password manager

An encrypted online or cloud-based program that generates, retrieves, and keeps track of random passwords across countless accounts and also protects information such as passwords, PINs, credit card numbers and their three-digit CVV codes, and answers to security questions.

Domain name

As it relates to an email address, this is the information that comes after the @ symbol—for example, schwab.com in jane.doe@schwab.com.

Spam filter

A program that detects unsolicited and unwanted emails and prevents them from reaching your email inbox. Usually these types of emails are instead sent to a spam folder.

Malware

Software that is intended to damage or disable computers and computer systems.

Learn more

- Visit these sites for more information and best practices:
- 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, https://www.fdic.gov/consumers/assistance/index.html.
- FBI Scams and Safety provides additional tips, https://www.fbi.gov/scams-and-safety.