Information Protection

Security and privacy of your confidential information is important to you and to us at Pothier Wealth Management. Know that we will always protect your data and other personal information. This information may be requested during a phone call with a Pothier Wealth Management customer service representative or upon registering for online account access.

Pothier Wealth Management is committed to safeguarding your personal and confidential information. We have provided some best practices that will help to enhance your security. Together we can work to protect what is most valuable to you.

Protect Your Account

Registering for online account access

- When you register for Pothier Wealth Management online account access, we will require several pieces of personal information from you, possibly including your product number, and/or Social Security number. This helps ensure that only you may register to access your own accounts.

- Avoid accessing your online accounts through publicly shared computers and Wi-Fi networks.

- Multi-Factor Authentication—The company provides clients with the option to add an extra layer of protection to their Pothier Wealth Management account login process by requiring entry of a security code in addition to your user name and password. The security code is a unique, single-use number you receive via phone call, text, or Google's Authenticator app.

Passwords

A strong password is important to protect your online accounts. When you are selecting a password, keep the following tips in mind:

Do

- Choose a long password of at least 8 characters. Longer passwords are more secure.
- Include upper–and lowercase letters, numbers, and symbols. This makes your password more difficult for someone to guess.
- Change passwords frequently.
- Consider using a password manager.
- Keep your password private.

Do not

- Do not use real names or your login name or any variation of it.
- Do not use Social Security numbers, words or numbers associated with easily attainable personal information, like birthdays, anniversaries, license plates, telephone numbers, or addresses.
- Do not use words from the dictionary.
- Do not use the same pattern for your passwords, such as smart1, smart2, etc.
- Do not write down your password or share your password with anyone else.
- Do not reuse passwords. Make sure you use different and unique passwords for all of your online accounts. Reusing a single password for multiple websites is never a good idea. If a cybercriminal obtains your password, they may try to use it on other websites.

Consider a password manager

Password management software, a virtual space that allows you to safely store your account usernames and passwords, can help simplify choosing and maintaining passwords for your online accounts. Make sure to keep your passwords updated within your password manager. Several password management applications are available for a variety of devices and operating systems. Check with a trusted technology expert to help you choose the appropriate password manager.

Stay Safe Online

Email hacking fraud

Email hacking occurs when a cybercriminal illegally gains access to an individual's email account. This allows the fraudster to read email messages and view the address book on the email account. Using this information, the cybercriminal (appearing to be the individual), contacts the individual's financial institutions via an email message and tries to obtain funds. Learn about how to protect yourself at Email Hacking Fraud. When email hacking occurs, emails can/will be intercepted and deleted by the fraudster, and the rightful sender and receiver will no longer see legitimate email traffic. If you believe a fraudster has accessed your email account, we recommend that you take the following actions to protect yourself:

- Never give your email address to anyone or any site that you do not trust.
- Never send personal or sensitive information in an unsecured email.

Identity theft

Printable Version

Identity theft occurs when someone wrongfully obtains another person's confidential information and uses that information, often for financial gain. Victims of identity theft may find their financial health seriously impacted and can spend months or years correcting the situation.

Consider the following to protect yourself in case your identity is stolen.

Protect your Pothier Wealth Management policies and accounts

Be prepared to provide your account/policy number when requesting the following:

- Life, Disability Income and Annuity—You can request a password to be used to verify your identity when you call the home office.
  - For Life and Disability Income Policies, call 1-917-410-4044.
  - For Annuities, call 1-917-410-4044.
- Long-Term Care—You can request additional authenticators be added to verify your identity when calling about your policy by calling 1-917-410-4044.
- Investment Accounts—You can request a note or block be added to your account.
  - For Pothier Wealth Management Investment Services and Pothier Wealth Management Wealth Management Company, including Trust and Private Client Services, call 1-917-410-4044 and ask for "investments."

Considerations for your other accounts

Remain vigilant—check your accounts often

- Get a copy of your credit report and review the accounts and other information provided. You can get a free credit report from AnnualCreditReport.com You're entitled to one free report from each of the credit reporting agencies every year.
- Review the account statements you receive each month from the banks and credit card companies you work with, and report anything that looks suspicious. If applicable, you are also entitled to receive copies of police reports if any have been filed.

Parental controls

Parental controls are available on most internet-enabled devices, like computers, smartphones, tablets, and gaming systems. When enabling parental controls, use age-appropriate settings to filter, monitor and block your child's activities. Work with a trusted technology expert if you have questions.

Secure Your Devices

Antivirus/anti-malware

Protect your computer from malicious software (malware) by installing and running up-to-date malware protection. A variety of options are available online or at local retail stores. Work with a trusted technology expert if you have questions.

Operating systems

To remain secure online, update your operating system (the system that manages the hardware and software on your computer and mobile devices) frequently. Consider activating automated updates if available. Apple, Google, Microsoft and other operating system vendors frequently update their operating systems. These updates may add functionality, increase security, and fix problems in existing software.
If you don't have a notification but want to check for software updates, search online for your device manufacturer and model number (example:*AT&T Samsung "model" software update*).

Apps

Be cautious when downloading applications (known as apps). Some apps may contain malware designed to steal your personal and financial information. Make sure that the updates or downloads come from the company that originally released the software. Safely download apps only from reputable, approved sites like Apple iTunes or Google Play.

To protect your privacy, review permissions at the time of installation or update to decide if you are comfortable granting access requested by that application.
Other applications such as Adobe Reader, iTunes and security software products also typically offer automatic update options. Turning on auto updates will ensure you always have the latest software version available. It's important to make sure you keep your applications updated to protect from vulnerabilities and increase functionality of services provided.

Using GPS on your mobile device

Your device's built-in global positioning system (GPS) locates and publishes information about your whereabouts. For example, applications like Facebook and Yelp allow you to "check in" at places using your mobile device, and then share your location on social networks.
Here are some tips to use GPS location services safely:

- Turn off GPS on your mobile device when you do not need it or only allow certain apps to use your location data. Refer to your mobile device manual for further instructions on how to adjust this feature.
- Know that what you share on one site may be linked to another site (such as Facebook and Twitter).
- Check the privacy settings on all your accounts. Make sure you are only sharing information with people you know.
- Remember when taking pictures with your mobile device that location information (known as geotagging) may be embedded in the photo.

For more information visit StaySafeOnline.org.

Physical security of mobile devices

Mobile devices include smartphones, tablets, laptops, cell phones, and other portable devices. They offer added convenience and flexibility. However, they do require additional protection. Treat your mobile devices as you would your wallet.
Consider the following best practices to keep your mobile devices secure:

- Always lock your screen when not in use. Locking your screen is a simple yet important thing you can do to ensure security on your mobile device, especially if it's lost or stolen.
- Beware of shoulder surfers—thieves who physically watch your onscreen activities to steal your confidential information or passwords. Pay attention to your surroundings and leave if you are uncomfortable.
- Never leave your mobile device unattended.
- If you are not able to keep your device with you, lock your mobile device in a secure location. If you need to leave your mobile device in your vehicle, lock it in the trunk out of sight; don’t leave it in the passenger compartment.

- Consider purchasing and using a cable lock to securely lock your laptop to immobile objects.

Web browsers

It is important to keep your web browsers up to date to correct any bugs or vulnerabilities that older versions may have. Download the latest version of your web browser. The following are examples of common web browsers:

- Chrome
- Firefox
- Internet Explorer
- Safari

If your web browser supports automatic updating, consider turning on that feature to ensure you always have the latest version.

Wi-Fi security

Wi-Fi allows you to wirelessly connect to the internet. The following tips can help you remain safe when you use Wi-Fi networks:

- Using a wireless network at home or using other internet enabled devices such as baby monitors, cameras, and thermostats is convenient, but leaving them unsecured is an opportunity for cybercriminals to hack in and discover sensitive information. Do not use any default settings or passwords provided by the manufacturer and make sure to add a unique passcode so that you and your family are the only ones accessing these devices.
- Realize that public Wi-Fi networks are not secure. Other people on the network may be able to view the information you send and receive unless that information is encrypted.

Web site security

- If you're performing a transaction or sharing confidential information through a website, make sure the site begins with https:// to ensure that the information will be secure during the transmission between your browser and the web site.
- If a site begins with anything other than https://, your information may be visible to other people. Never communicate confidential information through those type of sites.
- It's always best to go to a website via your saved favorites or by entering the website's URL in your browser window. Clicking on a link to a website inside an email or on a pop-up that displays on your screen could take you to a malicious site.
- Always log out of your accounts when you are finished if you're accessing those accounts from a computer that isn't your own.

Managing Your Records and Information

Managing your records and information appropriately will help keep you organized and in control of your confidential information. Properly disposing

of your records when you no longer need them will help protect your confidential information from falling into the wrong hands.

Records and information management

Government agencies like the Federal Trade Commission offer guidance on managing family and household records. Review the appropriate government agency's information to determine how long you should keep important documents. You should be securely disposing of confidential information on a regular basis.

Secure disposal

Properly disposing of your records will help prevent criminals sorting through your trash to locate your confidential information. Here are some tips for you to consider:

- Always shred your confidential information. Use a crosscut shredder that cuts the documents into small pieces.
- Shredders that cut documents into long spaghetti-like strands are not as secure. Properly motivated criminals can reconstruct those strands with enough effort.
- Shred DVDs, CDs, diskettes, tapes, and credit cards if possible. High"end shredders often have the capability to shred these items. Always confirm that a shredder can accommodate the items you want to shred.
- Before you sell a smartphone or mobile device, perform a factory reset to remove confidential information from the device.
- Use secure erase software to wipe, or electronically "shred," information on a personal computer's hard drive. At a minimum, take the hard drive out of a laptop or desktop computer before disposing of the old computer.
- Regularly delete emails from your Inbox and Deleted Items folder.

Pothier Wealth Management Information Security and Privacy Safeguards

Printable Version

The security and privacy of clients' confidential information are important to Pothier Wealth Management. The company takes its responsibility to protect this information seriously and uses technical, administrative, and physical controls to safeguard its data. The following are just some of the ways the company works to keep client information safe.

Technical

Pothier Wealth Management uses layers of technical controls to protect its clients' information:

- Antivirus: The company uses antivirus solutions to protect against malicious code that could compromise client information or damage company systems.

- Email filtering: The company actively filters incoming email messages for phishing and spam attacks.
- Encryption: The company encrypts client information accessed through online account access services to prevent unauthorized users from viewing that information. Company policies require client information stored on mobile devices used for business, including laptops, tablets, and smartphones, to be encrypted as well.
- Firewalls: The company uses robust firewall technologies to protect its internal network from unauthorized external parties gaining access.
- Fraudulent activity monitoring: The company monitors incoming email messages to help identify and prevent fraudulent financial requests.
- System activity monitoring: The company uses a variety of resources to monitor systems to identify suspicious activity. Intrusion detection systems and data leakage protection systems reduce the risk of incoming attacks and information loss.
- Multi-Factor Authentication: The company provides clients with an extra layer of protection to their Pothier Wealth Management account login process by requiring entry of a security code in addition to your user name and password. The security code is a unique, single-use number you receive via phone call, text, or Google's Authenticator app.

Administrative

Pothier Wealth Management supplements its technical controls with processes, procedures, and policies to further protect its clients' information:

- Authentication: The company requires multiple authentication factors to verify the identity of persons requesting policy, contract, or account information. A customer's right to policy, contract or account information follows state and federal regulations based on their role with the policy, contract or account.
- Business need to know: Access to company systems is granted on a business need to know basis. Only those people who need access to a given system and its information to accomplish their job responsibilities receive that access.
- Change control: The company uses a change control process to help ensure all changes to company systems maintain the confidentiality, integrity, and availability of those systems.
- Corporate governance: The company has a strong governance system with multiple committees supporting information protection initiatives.
- Cybersecurity threat simulations: The company conducts cybersecurity threat simulations to identify areas of program strength and opportunities for improvement.
- Incident response: The company maintains a well-defined computer security and privacy incident response program, designed to contain and resolve any incidents efficiently and effectively. The program is periodically reviewed and exercised to train and ensure preparation for events.

- Privacy: The entire workforce receives information protection training. An Enterprise Privacy team manages the privacy program for the company with the support of contacts across the organization.
- Internal and external IT auditors: The company's internal and external auditors regularly review and assess the company's information technology systems and operations.
- Policies and standards: The company maintains written policies and standards for information protection. These policies and standards provide the foundation and guidance for the company's information security, privacy, and risk management program.
- Records and information management and sanitization: The company maintains a records and information management program that manages the lifecycle of the company's information, including adherence to regulatory requirements and secure disposal of confidential information.
- Risk assessments: The company performs risk assessments during the development and acquisition of information systems to help ensure those systems include appropriate protection of client information.
- Security awareness: The company recognizes that end users are a critical component of an effective information security and risk management program. The company provides employees and financial representatives with security awareness and training, such as ongoing security awareness articles and events, training in company policies and standards, and simulated phishing exercises. Information to help clients protect themselves is also available on the company's corporate website.
- Separation of duties: The company separates specific job duties to prevent a conflict of interest when appropriate.
- Threat monitoring: The company works with internal teams and third-party industry security organizations to monitor its environment for existing and potential threats.
- User access reviews: The company regularly reviews user access to company systems to help ensure users maintain an appropriate level of access to those systems.

Physical

Pothier Wealth Management also protects its clients' information from physical harm and theft:

- Building and data center physical security: The company controls physical access to its buildings, data centers, and other facilities. Restricted access helps to ensure the confidentiality, integrity, and availability of company systems and physical assets within the company.
- Business continuity and disaster recovery planning: The company maintains and periodically tests defined business continuity and disaster recovery plans. These plans are designed to maximize the

availability of company systems and information and recover from natural or human-made disasters as efficiently and effectively as possible.

- Redundancy: As part of its business continuity and disaster recovery plans, the company maintains redundant data centers to help ensure the availability of company systems and client information.

Sending Securely

Pothier Wealth Management uses a secure system in order to protect confidential information that the company shares with clients via email. Replying to or forwarding messages that Pothier Wealth Management sends securely to your account may result in unsecure communications.
View the Secure Email Recipient Guide for additional details. Check with a trusted technology expert to discuss options for secure email for your own personal use.

Responsible Disclosure Policy

We want to hear from security researchers ("You" or "Your") who have information related to suspected security vulnerabilities ("Vulnerability" or "Vulnerabilities") of any Pothier Wealth Management services exposed to the internet. We value Your work and are committed to working with You. Please report Vulnerabilities to us in accordance with this Responsible Disclosure Policy ("Policy").

Pothier Wealth Management Box

Our financial representatives may also use a PWM Box account to facilitate secure sharing of documents with their customers or prospective clients.