Frequently Asked Questions

How does LPL Financial Secure my Information?

To protect your information and assets, LPL Financial employs extensive physical, technical, and procedural security controls at all of our facilities. We actively monitor and enforce compliance to our security policy and its related procedures. We regularly review, update, and modify our policies and procedures to respond to new threats and to adapt to changes in technology.

LPL Financial employees and customers receive thorough training in our security policy and are held accountable for adhering to the policy. Employees who work directly with customers also receive training in other related risks, such as identity theft.

Although we cannot fully disclose all that we do to protect the personally identifiable information of our customers, here are just a few measures we take:

- We employ strong authentication and password protocols.
- We enforce inactivity timeouts on our computers.
- We maintain and regularly test our firewalls.
- We continuously update our anti-virus and anti-malware protection.
- We employ threat monitoring/intrusion detection.
- We utilize encryption to protect our customer and employee data.
- We have mandatory training for employees, customers, and managed representatives.

How Can You Protect Your Own Information?

Protect your Social Security number.

Provide your Social Security number only when absolutely necessary, and do not carry your Social Security number with you.

Treat your trash and mail carefully.

To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, always shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.

Always deposit your outgoing mail containing personally identifying information in post office collection boxes or at your local post office rather than in an unsecured mailbox.

Be on guard when using the Internet.

The Internet can leave you vulnerable to online scammers, identity thieves, and more. For practical tips to help you be on guard against Internet fraud, secure your computer, and protect your personal information, visit www.OnGuardOnline.gov.

Verify a source before sharing information.

Don't give out personal information on the phone, through the mail, or over the Internet unless you've initiated the contact and are sure you know who you're dealing with. Identity thieves are clever and may pose as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information.

Avoid email hack attacks.

In the most serious cases, a compromised email account can lead not only to identity theft, but also to theft of your money. That's why one of the most important first steps you should take if your email account has been hacked is to notify your brokerage firm and other financial institutions. Take a look at the FINRA Podcast- Email Hack Attack? What Should You Do to find out the steps you should take if your email is hacked.

Questions related to the protection of your Social Security Number or your other personally identifiable information may be set to mailto: Security.mailbox@lpl.com.

How Can I Update and Correct my Personal Information?

Keeping your information accurate and up to date is very important. If your personal or account information is incomplete, inaccurate or not current, please contact your Financial Advisor or LPL Financial at (800) 558-7567.