LPL Privacy and Security FAQ

February 20, 2019

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 policies and 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 policies and are held accountable for adhering to the requirements. 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. Do not transfer funds without calling the known telephone number on file (not the number the cybercriminal provides) and receive confirmation. 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.

Use strong passwords or passphrases and protect your access credentials.
In order to help us protect your personal information, it is important that you always keep your account information safe. Never share your personal ID, password or PIN with anyone. You can also help keep your financial information secure by choosing a password that would be difficult for someone else to guess, preferably a longer password or passphrase that are not related to your job or personal life. Do not write your credentials down or leave them in a place where it might be discovered. We also recommend that you change your password regularly. If you have reason to believe your password may have been discovered, immediately change your password.

Are there risks from using services that aggregate my account information?
LPL does not recommend providing your login credentials or LPL account information to anyone else. Permitting others with access to your LPL accounts does increase the risk of fraudulent activity. That is why our online Terms and Conditions require that the person signing into an account must be the authorized account holder.

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 Investor Alert: Email Hack Attack?

Avoid phishing attacks.
Criminals send out fake emails that appear to be from real businesses, hoping to reach customers. These emails are called phishing emails. It's one of the ways criminals try to trick customers into giving personal information like account numbers and passwords. To help protect yourself from phishing emails you should never respond to emails requesting sensitive or confidential information, such as passwords, usernames, Social Security numbers, etc. Instead of clicking on links in emails, we advise you type website addresses directly into your browser. This will help further protect you from fraudulent links and phishing attempts. Never open an email attachment unless it comes from a trusted source.

How can I be sure I'm logging in to the real LPL website?

The best way to know that you are going to the real website is to type the URL directly in your browser or use favorites/bookmarks to access the website. Look for the https:// in the web address before you enter your username and password. It's OK for a home page to begin with "http," but you should always make sure you're on an "https" page before logging in. You can also read security details of sites by selecting the padlock icon located at the top or bottom of your browser window. View the security certificate and make sure it matches the site.

What should I do if I suspect fraud on one of my LPL accounts?

If you suspect you might be a victim of identity theft or financial fraud or receive a suspicious email or text purporting to be from LPL, contact our Security Hotline at (866) 578-7011 or email LPL security at 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.

How will I know if LPL updates the Consumer Privacy Notice or the Online Privacy Policy?

We will post a revised version of the Notice or Policy on the LPL website with a revised date at the top.

Questions related to the protection of your Social Security number or your other personally identifiable information may be sent to: Security.Mailbox@lpl.com.