LPL Financial

LPL Cyber Fraud Guarantee

LPL will reimburse clients for 100% of realized losses in your impacted LPL accounts, which were incurred directly as a result of unauthorized access to an LPL system.

**Please see below for terms and obligations.*

What is an "LPL System for purposes of this Guarantee?

An LPL system is a technology resource used for the organization, collection or processing of customer financial data, under the management and control of LPL Financial Holdings Inc.

What are protected losses?

Smishing is a form of phishing attack that is carried out by text or SMS message. Smishing attacks are similar to spear phishing attacks in which they often are created to look like a legitimate text message. The contents of the sent text messages often contain links that contain malware or instructions that are meant to trick users into revealing sensitive information. These attacks are particularly dangerous because people may be more inclined to trust a text message rather than an email. Many individuals are unaware that phishing attacks could be carried out via text message and these attacks can be just as dangerous as a traditional phishing email.

What is an "LPL System for purposes of this Guarantee?

An LPL system is a technology resource used for the organization, collection or processing of customer financial data, under the management and control of LPL Financial Holdings Inc.

What is not protected by this Guarantee?

- **Authorized access.** If you grant authority to, or share your LPL account access login information or credentials with any third party, their activity will be considered authorized by you. Transactions initiated by your LPL financial advisor or other third parties whom you have authorized to access your data are not protected.
- **Aggregator activity.** Activity resulting from access you grant to an aggregator is considered authorized and is not protected. An "aggregator" is a firm that collects, aggregates and presents financial account information to a customer. When you authorize an aggregator to access your LPL account information, the activities of the aggregator as well as its employees, agents and any third parties the aggregator does business with that receive your LPL account information, are considered to be authorized by you.
- **Other costs, fees, or indirect losses.** "Loss" does not include any tax consequences, legal fees, alleged trading or investment losses, or any other indirect losses or costs such as consequential damages.
- **Non-LPL accounts.** This guarantee only protects accounts that are within LPL's custody and control. It does not protect accounts and/or assets that are held or maintained by a third party (for example: 529 plans, annuity accounts, life insurance, TAMPs and any other direct business). LPL cannot be responsible for failure by third parties to protect your accounts and/or assets.

- **Beneficial Owners.** You must be the sole or joint owner of the protected LPL account to be covered by this guarantee. This guarantee does not apply to losses of cash or securities transferred to accounts that are beneficially owned by you.
- **Personal email compromise.** Email Security Incidents in which a customer's personal email is compromised may not be included in this guarantee depending on the circumstances.

Your Obligations – Your play a critical role in helping keep accounts secure and safe:

- Keep your personal identifying information and account information secure, and do not share your password, PIN, answers to security questions, or other information used to authenticate and gain access to your account(s).
- Never grant remote access to your computer or read back a one-time security password or authentication code unless you have initiated the service call to a phone number that you have verified to be valid. LPL will never contact you to ask for this information or to gain access to your computer.
- Use a unique username and password for your LPL accounts. If you are a victim of identity theft, change your password and notify us immediately. Please visit LPL Cyber Security and learn about more ways to protect your accounts.
- Regularly review your statements and account information to confirm account transactions and balances are valid and correct.
- You must immediately notify us of any suspected unauthorized account activity, errors, or discrepancies by contacting us at 1 (800) 558-7567.
- You must cooperate fully with LPL in investigating any suspected unauthorized activity, and in taking corrective measures to protect your account in the future.

If you have additional questions about the cyber fraud guarantee, please email security.mailbox@lplfinancial.com.