LPL Financial

<<Date>>

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address>>
<<City>> <<State>> <<Zip Code>>

Notice of Security Incident

Dear <<First Name>>:

We are writing to inform you of a cybersecurity incident experienced by LPL Financial LLC that affected your personal information. LPL Financial LLC is the broker-dealer and custodian for accounts maintained by a financial advisor who received your personal information in connection with providing financial advisory services to its clients. This notice describes the incident, the measures taken in response, and some steps you may consider taking to help protect your personal information.

What Happened?

Between September 30, 2025, and October 10, 2025, we learned of unauthorized securities transactions involving accounts maintained by clients of a small number of our affiliated financial advisors. We promptly contacted law enforcement and launched an investigation, with assistance from outside experts, to determine what occurred and to address the activity. Based on our investigation, we believe foreign threat actors gained access to the online accounts of certain affiliated financial advisors and used them in connection with a "hack pump-and-dump" trading scheme intended to artificially inflate the prices of securities. As part of this activity, and in the course of executing the scheme, we believe the threat actors may have been able to view certain of your personal information.

What Information Was Involved?

We have determined that the third party may have viewed the following personal information related to you: <<Variable Text *(Affected Data Elements)*>>.

What We Are Doing.

Upon discovery, we took steps to stop the unauthorized activity, restore any impacted accounts to their original securities holding positions, and secure all affected accounts. We also implemented new technical safeguards to strengthen our existing security controls and engaged outside information security and technology experts to assist in our review and investigation of the incident. After a thorough investigation, we have found no evidence of ongoing compromise to our information systems, including malware of any kind, and no evidence of additional unauthorized activity.

What You Can Do.

We wanted to make you aware of the incident so that you can take appropriate steps to protect your personal information and to offer you a complementary 24-month membership for credit monitoring and identity theft protection services through TransUnion. We encourage you to enroll in this service. We also encourage you to remain vigilant and review your account statements and free credit reports regularly to ensure there is no unauthorized or unexplained activity. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information.

We sincerely regret that this incident occurred and have taken measures to ensure that it does not happen again. Please contact us at (800) 558-7567 if you have any questions.

Sincerely,

Mona Nadim

Monda Nadim
Senior Vice President, Chief Privacy Officer & Associate General Counsel
LPL Financial LLC

Steps You Can Take to Help Protect Personal Information

Enroll in TransUnion's Monitoring Services

In response to this incident, we are providing you with access to **Single Bureau Credit Monitoring, Single Bureau Credit Report, and Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Variable Text *(Registration Code)*>>.

In order for you to receive the monitoring services described above, you must enroll within 120 days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus: Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call 1-877-322-8228 toll-free. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" at no charge on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

	Equifax	**Experian**	**TransUnion**
URL	https://www.equifax.com/personal /credit- report services/	https://www.experian.com/ help/	https://www.transunion.com/ credit-help/
Phone	1-888-298-0045	1-888-397-3742	1-800-916-8800
Fraud Alert	Equifax Information Services LLC P.O. Box 105069, Atlanta, GA 30348-5069	Experian P.O. Box 9554, Allen, TX 75013	TransUnion P.O. Box 2000, Chester, PA 19016
Credit Freeze	Equifax Information Services LLC P.O. Box 105788, Atlanta, GA 30348-5788	Experian Security Freeze P.O. Box 9554, Allen, TX 75013	TransUnion P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the three major credit reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and https://ag.ny.gov. The New York Department of State Division of Consumer Protection may be contacted at: 1-800-697-1220 and https://dos.ny.gov/consumer-protection.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6000; and https://ncdoj.gov/contact-doj.