



<<Date>>

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

<<Variable Text (Notice of [Data Breach / Security Incident])>>

Dear <<First Name>>:

We are writing to inform you of a cybersecurity incident experienced by LPL Financial LLC that may have 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 November 20, 2025, and November 25, 2025, we learned of unauthorized securities transactions and financial transfers 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. Our investigation found that malware distributed through phishing messages affected a limited number of individual advisor devices and resulted in unauthorized third-party access to the accounts of those advisors on LPL's web-based advisor portal. Our investigation did not identify evidence that your sensitive personal information was accessed or acquired by a third party in connection with these events. However, we are notifying you out of an abundance of caution because we cannot rule out the possibility that a third party may have viewed certain of your personal information in the course of executing the scheme.

What Information Was Involved?

A 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 financial 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 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 complimentary 24-month membership for credit monitoring and identity theft protection services through Experian. 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 [Experian to provide call center number] if you have any questions.

Sincerely,

Mona Nadim
Vice President, Interim Chief Privacy Officer & Associate General Counsel
LPL Financial LLC

Steps You Can Take to Help Protect Personal Information

Enroll in Experian's Monitoring Services

[Insert Experian text for 24-month credit monitoring and identity theft protection services]

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
<i>URL</i>	https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help/
<i>Phone</i>	1-888-298-0045	1-888-397-3742	1-800-916-8800
<i>Fraud Alert</i>	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
<i>Credit Freeze</i>	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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is

limited; consumers must give consent for credit reports to be provided to employers; consumers may limit “prescreened” offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the New York State 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; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. The Oregon Attorney General may be contacted at 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and <https://www.doj.state.or.us/>. For more information on security locks, you can visit the “Place a credit freeze” page on the Oregon Division of Financial Regulation website at <https://dfr.oregon.gov/financial/protect/pages/place-credit-freeze.aspx>.

For Vermont residents, helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General’s website at <http://www.ago.vermont.gov>. If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General’s Office at 1-802- 656-3183 (1-800-649-2424 toll free in Vermont only).