



Justin Schiff
Office: (267) 930-4256
Fax: (267) 930-4771
Email: jschiff@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 25, 2025

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Lighthouse Wealth Partners (“LWP”) located at 3945 Market Street Wilmington, NC 28403, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately three (3) Maryland residents. By providing this notice, LWP does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

LWP recently became aware of suspicious activity related to an employee email account. LWP immediately took steps to secure the email account and launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. Through the investigation, LWP determined that there was unauthorized access to the affected email account at various times between June 20, 2024, and July 25, 2024, and that the unauthorized actor was potentially able to view or download files contained within the email account.

Upon becoming aware of the unauthorized access, LWP undertook a diligent and comprehensive review process to identify sensitive information that may have been contained within the impacted email account, and to identify the individuals whose information may have been impacted. Those efforts were recently completed, and LWP provided written notification to individuals whose information was contained within the impacted email account.

The information that could have been subject to unauthorized access includes name, Social Security number and financial account information.

Notice to Maryland Residents

On or about March 25, 2025, LWP provided written notice of this incident to approximately three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, LWP moved quickly to investigate and respond, assess the security of LWP systems, and identify potentially affected individuals. LWP is also working to implement additional safeguards and training to its employees. LWP is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

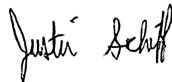
Additionally, LWP is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. LWP is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, and the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

LWP is also providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4256.

Very truly yours,

A handwritten signature in black ink, appearing to read "Justin Schiff".

Justin Schiff of
MULLEN COUGHLIN LLC

JXS/sph
Enclosure

EXHIBIT A

P.O. Box 989728
West Sacramento, CA 95798-9728

<<Name 1>> <<Name 2>>
<<Address 1>><<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

March 25, 2025

NOTICE OF <<Variable Data 2>>

Dear <<Name 1>> <<Name 2>>:

Lighthouse Wealth Partners (“LWP”) writes to inform you of an event that may impact the privacy of some of your information. Although we are unaware of any identity theft or fraud occurring as a result of this event, we are providing you with this notice in an abundance of caution, to inform you of the event, our response, and steps you may take to help protect your information, should you feel it necessary to do so.

What Happened? LWP recently became aware of suspicious activity related to an employee email account. We immediately took steps to secure the email account and launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that there was unauthorized access to the affected email account at various times between June 20, 2024 and July 25, 2024 and that the unauthorized actor was potentially able to view or download files contained within the email account.

Upon becoming aware of the unauthorized access, LWP undertook a diligent and comprehensive review of the process to identify sensitive information that may have been contained within the impacted email account, and to identify the individuals whose information may have been impacted. Through that review, LWP determined that certain information related to you was contained within the potentially affected files. Therefore, LWP is providing you with notification in an abundance of caution.

What Information Was Involved? The review determined that the following types of information related to you were found in the impacted email account: your name, <<Variable Data 1>>. Please note that LWP is not aware of any attempted or actual misuse of your information, or that your information was used to commit identity theft or fraud.

What We Are Doing. The confidentiality, privacy, and security of information within our care is among our highest priorities. Upon learning of the event, we promptly took steps to secure our email environment and investigate the activity. We are reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar events moving forward. We are also notifying potentially impacted individuals, including you, so you may take steps to better protect your information, should you feel it is appropriate to do so.

As an added precaution, we are also offering you immediate access to credit monitoring and identity theft protection services for <<Membership Offering Length>> months at no cost to you, through IDX, the data breach and recovery services expert. You can find information on how to enroll in these services in the enclosed *STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION*. We encourage you to enroll in these services as we are not able to do so on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also enroll in the complimentary credit monitoring services we are offering. Please also review the information contained in the enclosed *STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact IDX at 1-800-939-4170 Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is June 25, 2025. You may also write to us at 3945 Market Street, Wilmington, NC 28403. We take this event very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,
Lighthouse Wealth Partners

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit 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, toll-free, 1-877-322-8228. 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 1-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” 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
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their 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; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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 www.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 Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 0 Rhode Island residents that may be impacted by this event.