



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

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

August 16, 2024

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 Highlands CPA, LLC (“Highlands”) located at 2700 E. Louisiana Avenue, Unit 102, Denver, Colorado 80210, and are writing to notify your office of an incident that may affect the security of certain personal information relating to four (4) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Highlands 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

On May 23, 2024, Highlands became aware of suspicious activity on its network that could have been related to fraudulent tax filings on behalf of certain clients. Highlands immediately took steps to secure its systems and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that an email account and file transfer applications used by Highlands were subject to unauthorized access between May 2, 2024 and May 21, 2024 and that certain files were thus acquired by an unknown actor during the period of unauthorized access. In response, Highlands undertook a thorough review of the data determined to be at risk to assess the type of information at issue and to whom that information relates. On July 31, 2024, Highlands determined information related to certain individuals could be affected. The information that could have been subject to unauthorized access includes name, Social Security number, and financial account information.

Notice to Maryland Residents

On August 16, 2024, Highlands provided written notice of this incident to four (4) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**. Highlands also provided an initial wave of notice to individuals on June 25, 2024, but it did not include any Maryland residents.

Other Steps Taken and To Be Taken

Upon discovering the event, Highlands moved quickly to investigate, assess the security of its systems, and identify potentially affected individuals. Further, Highlands notified federal law enforcement regarding the event and is working to implement additional safeguards and training to its employees. Highlands is also providing individuals whose personal information was potentially affected by this incident access to credit monitoring services for twelve (12) months through Experian at no cost to the individuals.

Additionally, Highlands 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. Highlands is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. Highlands is providing written notice of this incident to 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) 930-4259.

Very truly yours,

A handwritten signature in black ink, appearing to read "Colin D. Scanlon".

Colin D. Scanlon of
MULLEN COUGHLIN LLC

EXHIBIT A



Return Mail Processing
PO Box 999
Suwanee, GA 30024

2 1 398 *****SNGLP

SAMPLE A. SAMPLE - L03



APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



August 16, 2024

NOTICE OF [EXTRA1]

Dear Sample A. Sample:

Highlands CPA, LLC (“Highlands”) writes to notify you of an incident that may affect some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your information should you feel it appropriate to do so.

What Happened? On May 23, 2024, Highlands became aware of suspicious activity on its network that could have been related to fraudulent tax filings on behalf of certain clients. We immediately took steps to secure our systems and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined that an employee email account and file transfer applications used by Highlands were subject to unauthorized access between May 2, 2024 and May 21, 2024 and that certain files were thus acquired by an unknown actor during the period of access. In response, Highlands undertook a thorough review of the data determined to be at risk, with the assistance of third-party data review specialists, to assess the type of information at issue and to whom that information relates. On July 31st, 2024 Highlands determined information related to you was subject to unauthorized access.

What Information Was Involved? The information that could have been impacted by this incident includes your [Extra2] and name.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon discovering the suspicious activity, we immediately commenced an investigation to confirm its nature and scope. We also reported the event to law enforcement and implemented additional security measures related to data privacy and security.

As an added precaution, we are offering you access to credit monitoring and identity theft protection services for [Extra3] months through Experian at no cost to you. The deadline to enroll in these services is November 29, 2024. A description of services and instructions regarding how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information*. Please note that you must complete the enrollment process yourself as we are not permitted to enroll you in these services.

What You Can Do. In addition to enrolling in the credit monitoring being offered to you, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and reporting suspected identity theft and fraud to your credit card company or bank. You may also review the information contained in the enclosed *Steps You Can Take to Protect Personal Information*. There you will also find more information regarding ways to protect and monitor your information.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have questions or concerns, or would like an alternative to enrolling in the services being offered online, please call 855-879-2743, toll-free, Monday through Friday from 8:00 am - 8:00 pm CST (excluding major U.S. holidays). Be prepared to provide your engagement number [Engagement Number]. You can also write to us at Highlands CPA, LLC at 2700 E. Louisiana Ave, Unit 102, Denver, CO 80210.

Sincerely,

A handwritten signature in dark ink, appearing to read "Taylor McIlvennan", with a long, sweeping horizontal line extending to the right.

Taylor McIlvennan
Highlands CPA, LLC

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra3] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** November 29, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 855-879-2743 by November 29, 2024. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Register for the IRS Identity Protection PIN Program

The IRS offers an Identity Protection PIN Program to individuals as protection against fraudulent tax filings. An Identity Protection PIN (IP PIN) is an assigned six-digit number that prevents someone else from filing fraudulent federal income tax returns using your Social Security number. The IP PIN is known only to you and the IRS and helps to verify your identity when you file your electronic or paper tax return. For more information about the IRS IP PIN program, please visit <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

To register for an IP PIN on www.irs.gov, please follow the below step-by-step instructions:

1. Go to www.irs.gov
2. Click on “View Your Account”
3. Click “Create or view your account”
4. Click “Create Account”

For the “Create Account” step, in addition to your name, social security number, date of birth, and address you will need:

- An email account you can readily access
- A cell phone that can receive text messages from
- Financial information, such as a credit card number, mortgage loan number, student loan number to verify your identity

Important – Each taxpayer must have their own account (so spouses each must register for their own accounts)

5. Once you create your account and log in:

- At www.irs.gov, search “Get an IP Pin.” Log into your account and choose a PIN. Print the page for your records. Each tax filing season you will need to log into the account to get the PIN for that filing season. You cannot file your return without the PIN.

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.