Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

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

October 1, 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 MHTax located at 508 Oak Road, Merion Station, PA 19066, and are writing to notify your office of an incident that may involve certain personal information relating to one (1) Maryland resident. By providing this notice, MHTax 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 July 5, 2024, MHTax discovered suspicious activity within an email account that included the sending of phishing emails. MHTax quickly took steps to confirm the suspicious activity, and with the assistance of third-party forensic specialists, began an investigation to determine the nature and scope of the activity. MHTax determined that an unauthorized actor gained access to the email account and could have obtained a copy of the entire email account. While MHTax has protocols for exchanging personal information through the use of secure portals and not through email, it is possible that MHTax may have received emails containing personal information. As a result, and out of an abundance of caution, MHTax initiated an internal review to determine the names and addresses of all of its clients. MHTax completed this review on July 19, 2024.

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

Notice to Maryland Resident

On or about October 1, 2024, MHTax provided written notice of this incident to one (1) Maryland resident. 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 discovering the event, MHTax moved to investigate and respond to the incident, assess the security of MHTax systems, and identify potentially affected individuals. MHTax is also working to implement additional safeguards. MHTax is providing access to credit monitoring services for twelve (12) months through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MHTax is providing impacted individuals with guidance on how to better protect against identity theft and fraud, MHTax 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.

MHTax is 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) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/mah
Enclosure

EXHIBIT A

MHtax Crossborder
Return Mail Processing
PO Box 999
Suwanee. GA 30024

1 1 1 ************************************SNGLP
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789
usa

October 1, 2024

NOTICE OF [Extra1]

Dear Sample A. Sample:

MHTax is writing to notify you of an event that may involve some of your personal information. You are receiving this letter because you are a current or former tax preparation client of MHTax. We write to provide you with information about the event, our response, and steps you can take to help protect against the possible misuse of your information, should you feel it is appropriate to do so.

What Happened? On July 5, 2024, MHTax discovered suspicious activity within an email account that included the sending of phishing emails. MHTax quickly took steps to confirm the suspicious activity, and with the assistance of third-party forensic specialists, began an investigation to determine the nature and scope of the activity. MHTax determined that an unauthorized actor gained access to the email account and could have obtained a copy of the entire email account. While MHTax has protocols for exchanging personal information through the use of secure portals and not through email, it is possible that MHTax may have received emails containing personal information. As a result, and out of an abundance of caution, MHTax initiated an internal review to determine the names and addresses of all of its clients. MHTax completed this review on July 19, 2024. MHTax is notifying you because its investigation determined that there is a possibility that personal information related to you was contained within the email account at the time of this event.

What Information Was Involved? Your name, address, Social Security number and financial account information could possibly be accessible in the email account if you sent it to MHTax via email. We have no evidence that any of your information was used for identity theft or fraud as a result of this event.

What We Are Doing. We take this incident and the obligation to safeguard the information in our care very seriously. After discovering the suspicious activity, we promptly took steps to contain the issue and engage with a third-party forensic specialist to assist in conducting a comprehensive investigation. Further, as part of our ongoing commitment to the privacy and security of personal information in our care, we are reviewing and enhancing existing policies and procedures relating to data protection and security. We have instituted additional security measures to better protect against future similar events.

MHTax has no evidence of fraud or identity theft as a result of this event, however, out of an abundance of caution, we are notifying you and providing information and resources to assist you in helping to protect your personal information, should you feel it appropriate to do so. As an added precaution, we are offering you access to credit monitoring and identity theft protection services for [Extra2] months through Experian at no cost to you. If you wish to activate these complimentary services, you may follow the instructions included in the attached *Steps You Can Take to Help Protect Personal Information.* We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should report any fraudulent activity to law enforcement. You can also enroll to receive the complimentary credit monitoring services that we are offering to you. Please also review the information in the enclosed *Steps You Can Take to Help Protect Personal Information.*

For More Information. If you have additional questions or concerns, please feel free to call us at 833-931-6200. We are available Monday through Friday, from 8am - 8pm Central Time (excluding U.S. holidays). You may also write MHTax at 508 Oaks Rd, Merion Station, PA 19066.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Marina Hernandez

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [Extra2] 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 [Extra2] 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 [Extra2]-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 833-931-6200 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 [Extra2]-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 ExtendCARE™:** 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.

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.

Identity Protection PIN

Opt-In Program for Taxpayers

IRS

WHAT'S NEW **You are now eligible to voluntarily get an Identity Protection PIN that will help protect you from tax-related identity theft.**

What is the IP PIN?

The IP PIN is a 6-digit number assigned to eligible taxpayers. It helps prevent identity thieves from filing fraudulent tax returns with stolen Social Security numbers (SSNs). An IP PIN helps the IRS verify taxpayers' identities and accept their electronic or paper tax returns for processing. The IRS issues IP PINs to confirmed identity theft victims once their cases are resolved. This process is unchanged. What is new is that any taxpayers who wants an IP PIN, even if they are not victims of identity theft, may now obtain one.

About the IP PIN Opt-in Program

Here's what you need to know before applying for your IP PIN:

- This is a voluntary program.
- You must pass a rigorous identity verification process.
- Spouses and dependents are eligible for an IP PIN if they can verify their identities.
- An IP PIN is valid for a calendar year.
- A new IP PIN is generated each filing season, which you must obtain using the online tool.
- The IP PIN tool is unavailable generally mid-November through mid-January each year.
- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.

How to Get an IP PIN

The fastest, easiest and preferred way is by using the Get an IP PIN online tool. Here's how it works:

- Go to **IRS.gov/IPPIN**, select the Get an IP PIN tool, verify your identity and create an account
- Your IP PIN will be revealed to you.

Can't pass online identity proofing?

There are alternatives but there will be a delay in obtaining an IP PIN. Here's how it works:

- File Form 15227 if you have a valid SSN or ITIN, an adjusted gross income on your last filed return is below $79,000 for individuals or $158,000 for Married Filing Joint and access to a telephone. An IRS assistor will call you, validate your identity and ensure that you receive an IP PIN the next filing season.
- If you are ineligible for Form 15227, you may schedule a visit at a Taxpayer Assistance Center to request an IP PIN. You can find the TAC office closest to you with our **Taxpayer Assistance Locator** tool or call (844-545-5640) to schedule an appointment..

IMPORTANT: The IRS will never email, text or call you to request your IP PIN. Do not reveal your IP PIN to anyone but your trusted tax software provider or tax preparer. Neither your provider nor preparer will ask for your IP PIN except to complete your tax return. Protect your IP PIN from theft, especially scams.

Elección de entrar al Programa del *IP PIN*

para los contribuyentes

IRS

QUÉ HAY DE NUEVO **Ahora usted es elegible para obtener voluntariamente un Número de Identificación Personal (*PIN*, por sus siglas en inglés) para la Protección de la Identidad que lo ayudará a protegerse del robo de identidad relacionado con los impuestos.**

¿Qué es el *IP PIN*?

El Número de Identificación Personal para la Protección de la Identidad (*IP PIN*, por sus siglas en inglés) es un número de seis dígitos que se asigna a los contribuyentes elegibles. Este número ayuda a evitar que los ladrones de identidad presenten declaraciones de impuestos fraudulentas con números de Seguro Social (*SSN*, por sus siglas en inglés) robados. Un *IP PIN* ayuda al Servicio de Impuestos Internos (*IRS*, por sus siglas en inglés) a verificar la identidad de los contribuyentes y a aceptar sus declaraciones de impuestos electrónicas o en papel para su trámite. El *IRS* emite los *IP PIN* a las víctimas de robo de identidad confirmadas, una vez que se resuelven sus casos. Este proceso no ha cambiado. Lo que es nuevo es que todos los contribuyentes que deseen un *IP PIN*, pueden ahora obtener uno aunque no sean víctimas de robo de identidad.

Acerca de entrar al Programa del *IP PIN*

Lo siguiente es lo que tiene que saber antes de solicitar su *IP PIN*:

- Este es un programa voluntario.
- Usted debe aprobar un proceso riguroso de verificación de la identidad.
- Los cónyuges y los dependientes son elegibles para un *IP PIN* si pueden verificar sus identidades.
- Un *IP PIN* es válido para un año calendario.
- Se genera un nuevo IP PIN cada temporada de presentación, que usted debe obtener utilizando la herramienta en línea.
- La herramienta del *IP PIN* no está disponible generalmente de mediados de noviembre a mediados de enero de cada año.
- Los *IP PIN* se tienen que anotar correctamente en las declaraciones de impuestos electrónicas y en papel para evitar rechazos y demoras.

Cómo obtener un *IP PIN*

La manera más rápida, fácil y preferida de obtener un *IP PIN* es utilizando la herramienta en línea Obtenga un *IP PIN* (en inglés). Así es como funciona:

- Visitar **IRS.gov/es/IPPIN**, seleccionar la herramienta Obtenga un *IP PIN* (en inglés), verificar su identidad y crear una cuenta
- Se le revelará su *IP PIN*.

¿No puede pasar la prueba de identidad en línea?

Existen alternativas, pero habrá un retraso para obtener un IP PIN. Así es como funciona:

- Presente el Formulario 15227 si tiene un *SSN* válido o un *ITIN*, un ingreso bruto ajustado en su última declaración presentada es menos de $79,000 para individuos o $158,000 para casados con presentación conjunta, y tiene acceso a un teléfono. Un asistente del *IRS* lo llamará, verificará su identidad y se asegurará de que usted reciba un *IP PIN* la próxima temporada de presentación de impuestos.
- Si usted no es elegible para el Formulario 15227(sp), puede programar una visita a un Centro de Asistencia al Contribuyente (TAC, por sus siglas en inglés) para solicitar un IP PIN. Puede encontrar la oficina del TAC más cercana a usted con nuestra **herramienta Localizador de Asistencia al Contribuyente** o llamar al (844-545-5640) para programar una cita.

IMPORTANTE: El *IRS* nunca le enviará correos electrónicos, ni mensajes de texto ni le llamará para solicitar su *IP PIN*. No revele su *IP PIN* a nadie excepto a su proveedor de software de impuestos o preparador de impuestos de confianza. Ni su proveedor ni su preparador le pedirán su *IP PIN* excepto para completar su declaración de impuestos. Proteja su *IP PIN* del robo, especialmente de las estafas.

Publication 5367(EN-SP) (Rev. 3-2024) Catalog Number 73362D Department of the Treasury **Internal Revenue Service** www.irs.gov