



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Alexandria N. Murphy
Office: (267) 930-1345
Fax: (267) 930-4771
Email: amurphy@mullen.law

40 Burton Hills Boulevard, Suite 200
Nashville, TN 37215

June 27, 2022

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

Dear Sir or Madam:

We represent Solomon & Company CPA, Inc. ("Solomon & Company"), located at 60 Dedham Avenue, Suite 202, Needham, MA 02492, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Solomon & Company 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 April 8, 2022, Solomon & Company learned that an unauthorized actor fraudulently filed tax returns for a limited number of Solomon & Company clients. Upon learning of this incident, Solomon & Company quickly launched an investigation to determine whether there was a compromise of any Solomon and Company systems and, if so, what data was at risk. On or about May 19, 2022, the investigation determined that an unknown actor accessed certain areas of Solomon & Company's systems containing taxpayer records between April 7, 2022 to April 9, 2022. Solomon & Company reviewed the systems potentially accessible to the unknown actor for sensitive information, and the review was completed on June 6, 2022.

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 June 27, 2022, Solomon & Company 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, Solomon & Company moved quickly to investigate and respond to the incident, assess the security of Solomon & Company systems, and identify potentially affected individuals. Further, Solomon & Company notified federal and state taxation authorities regarding the event. Solomon & Company is also working to implement additional safeguards and training to its employees. Solomon & Company is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Solomon & Company 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 the Internal Revenue Service and individuals' credit card company and/or bank. Solomon & Company 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1345.

Very truly yours,

Alexandria N. Murphy of
MULLEN COUGHLIN LLC

ANM/dle
Enclosure

EXHIBIT A

<<Insert Solomon letterhead>>

<<Return Mail Address>>

<<First Name>> <<Middle Name/Initial>> <<Last Name>>

<<Address 1>>

<<Address 2>>

<<Date>>

<<City>>, <<State>> <<Zip>>

Re: Notice of <<Variable Header>>

Dear <<First Name>> <<Middle Name/Initial>> <<Last Name>>:

Solomon & Company CPA, Inc. ("Solomon & Company") is writing regarding a recent incident that may affect the security of some of your information provided to us for tax filing purposes. This notice provides additional information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On April 8, 2022, Solomon & Company learned that an unauthorized actor fraudulently filed tax returns for a limited number of Solomon & Company clients. Upon learning of this incident, we quickly launched an investigation to determine whether there was a compromise of any Solomon and Company systems and, if so, what data was at risk. On or about May 19, 2022, the investigation determined that an unknown actor accessed certain areas of our systems containing taxpayer records between April 7, 2022 to April 9, 2022. We reviewed the systems potentially accessible to the unknown actor for sensitive information, and on June 6, 2022, we completed our review.

What Information Was Involved? We determined the following types of information relating to you were present in the affected systems: <<data elements>>, and name.

What We Are Doing. The confidentiality, privacy, and security of client information is one of our highest priorities. Upon learning of this incident, we moved quickly to investigate, respond, and assess the security of our systems. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards. We are working with any clients whose returns may have been rejected to file their tax returns. Additionally, we contacted the Internal Revenue Service (IRS) and state tax authorities about this incident.

We are also offering you access to complimentary credit monitoring services for 12 months through Experian. If you wish to activate these services, you may follow the instructions included in the *Steps You Can Take to Protect Personal Information*.

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 over the next twelve (12) to twenty-four (24) months. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. There you will also find more information on the complimentary credit monitoring services we are making available to you. While Solomon & Company will cover the cost of these services, you will need to complete the activation process. If you become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you should file the IRS Form 14039 Identity Theft Affidavit along with a paper copy of your return and mail according to the instructions on that form. A copy of this form can be found at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf> or <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call Solomon & Company at (781) 828-7036, 8am – 5pm ET. Solomon & Company takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

<<Insert Laurie Signature Image>>

Laurie Solomon, CPA
President

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Complimentary Credit Monitoring Services:

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: [code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332 by **September 30, 2022**. Be prepared to provide engagement number **B054732** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-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 agents 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.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. 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 (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 this Identity Restoration support is available to you for 12 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. You will also find self-help tips and information about identity protection at this site.

* 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 “Sign in to Your Account”
3. Click “Sign in to your Online Account”
4. If you do not have an existing account, click “Create Account” or, if you do have an account, follow the steps to sign in with an existing 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 from which you can receive text messages
- Financial information, such as a credit card number, mortgage loan number, student loan number to verify your identity

Important – Each taxpayer must have his/her 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. Once created, you cannot file your return without the PIN.

Monitor Your Accounts

Tax Return Guidance. You can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state’s tax authority, visit <http://www.taxadmin.org/state-tax-agencies>.

Credit Reports. 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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
888-298-0045	1-888-397-3742	833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

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 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, you have the right to obtain any police report filed in regard to this incident. There are two (2) Rhode Island residents impacted by this incident.