Mohr CPAs LLP
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003

Mohr CPAs LLP

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip

November xx, 2023

NOTICE OF SECURITY INCIDENT

Dear <<FirstName>> <<LastName>>:

Mohr CPAs LLP ("Mohr CPAs") is writing to notify you of an incident that we determined may have impacted the privacy of some of your information. This letter provides an overview of the incident, our response, and resources available to you to help protect your information, should you wish to do so.

What Happened? On or about September 29, 2023, Mohr CPAs discovered suspicious activity related to a member of the firm's email account. Shortly thereafter, Mohr CPAs received notifications that tax e-filings for certain clients were rejected and flagged as fraudulent. We immediately launched an internal investigation to determine whether an issue occurred on our systems that may have resulted in the fraudulent tax filings. Additionally, we worked with third-party forensic specialists to perform a thorough investigation. On October 23, 2023, we determined that a server in Mohr CPAs' environment was accessed by an unauthorized party on or about September 29, 2023, and that a portion of the files stored on that server were exfiltrated by an unauthorized actor. While not all files on the impacted server were subject to unauthorized access and exfiltration, we were not able to identify precisely which files were accessed and exfiltrated. Since the affected server contained information relating to our clients and their dependents, we are notifying all current and former clients, as well as their spouses and dependents, whose information was stored on the impacted server in an abundance of caution, including you, because it is possible your information was affected. If your tax e-filing was rejected as fraudulent, we have contacted you directly.

What Information Was Involved? Our investigation determined the information potentially impacted includes your name, Social Security number, date of birth, and Driver's license number, and may include other information such as personal account information shown on government forms, if such information was provided to Mohr CPAs in order to prepare your tax return. If information of your spouse or dependent(s) was involved, we are providing separate notifications to you for each dependent.

What We Are Doing. We take this incident and the security of information in our care seriously. Upon learning of this incident, we moved quickly to investigate and respond, and worked to secure our environment. We have also been in communication with the Internal Revenue Service, Wisconsin Department of Revenue, and the Federation of Tax Associates and have cooperated with these agencies'

investigations. As part of our ongoing commitment to the security of information, we are also reviewing and enhancing existing policies and procedures to help prevent a similar future incident.

We are also offering you access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for <<service length>> from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. More information about these services is below. If you wish to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Help 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. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information.* There you will also find more information on the complimentary credit monitoring services we are making available to you. While Mohr CPAs will cover the cost of these services, you will need to enroll yourself in the services we are offering, if you would like to do so, as we are unable to enroll you on your behalf.

Additionally, we encourage you to apply for an Identity Protection PIN through the IRS. Instructions for applying for an Identity Protection PIN can be found in the attached *Steps You Can Take to Help Protect Personal Information.* Please note that the IP PIN system will be down until mid-January as part of the IRS standard maintenance policy; however, you can start the process of obtaining an IP PIN now by visiting www.irs.gov/ippin and creating an ID.me account. We suggest you apply for an IP PIN as soon as possible in January so you have it before the filing season starts on January 23, 2024.

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 our dedicated assistance line at 1-833-961-6767, Monday through Friday from 8:00 a.m. to 8:00 p.m. E.S.T. (excluding U.S. holidays).

We sincerely apologize that this incident occurred and regret any inconvenience or concern it may have caused you.

Sincerely,

Mohr CPAs LLP

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/mohrcpa** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<unique code>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Apply for an Identity Protection PIN

The voluntary Identity Protection PIN tool is available in all 50 states. To be eligible for 2023, you must have filed a federal return last year. To apply, visit www.irs.gov/ippin.

How to apply:

- Taxpayers may go to the Get an IP PIN tool on IRS.gov, pass Secure Access authentication and immediately access a six-digit IP PIN.
- Do not file a Form 14039, Identity Theft Affidavit, if you are not a tax-related identity theft victim and you are voluntarily opting into the program.
- When prompted by tax preparation products, clients or their tax preparers must enter the IP PIN issued to the primary and/or secondary taxpayers or their dependents.
- An electronic return without a correct IP PIN will be rejected; paper returns will be subject to greater scrutiny.
- Taxpayers with either a Social Security number (SSN) or Individual Tax Identification Number (ITIN) who can verify their identities are eligible.
- An IP PIN is valid for one calendar year. Clients must obtain a new IP PIN each year at the start of the filing season by accessing the account they created at www.irs.gov/ippin.
- While currently there is no opt-out feature, the IRS is looking to add this feature later for taxpayers with online access.

Alternatives to online Get an IP PIN tool:

- Taxpayers who cannot authenticate their identities online and who made $72,000 or less may file Form 15227. An IRS assistor will call taxpayers to ask a series of questions to verify their identities. An IP PIN will be issued at the start of the next calendar year.
- Taxpayers who cannot authenticate online and who made more than $72,000 will have an option, still being vetted, to verify their identities in person at a local IRS office. An IP PIN will be issued within 3 weeks if their identity is authenticated at a local office.

No change for victims of tax-related identity theft:

- File a Form 14039 if your e-filed return rejected because of a duplicate SSN filing; mail it with your paper tax return. If your 2022 tax return rejected, Mohr CPAs has already done this for you.
- The IRS will investigate the case and remove the fraudulent return.
- Once the case is resolved, you will automatically receive an IP PIN via postal mail at the start of the next calendar year.
- Confirmed identity theft victims may not opt-out of the IP PIN program because of known risks.

Please note that the IP PIN system will be down until mid-January as part of the IRS standard maintenance policy; however, you can start the process of obtaining an IP PIN now by visiting www.irs.gov/ippin and creating an ID.me account. We recommend you apply for an IP PIN as soon as possible in January so you have it before the filing season starts on January 23, 2024.

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 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 security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number or copy of Social Security card;
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	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

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.marylandattorneygeneral.gov. Mohr CPA is located at 10361 Innovation Drive, Suite 150, Milwaukee, WI 53226.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.