

Good afternoon,

This firm represents Horner, Wible & Terek PC, (HWT) a tax preparation service provider in Pennsylvania. Pursuant to the Maryland Personal Information Protection Act, we are hereby notifying you of a data breach that occurred at the firm. As required, please find attached redacted copies of the two letters that will be mailed out, one for adults and one for minors.

In brief, a forensic investigation revealed that malware had been installed on a firm computer that had access to its clients' personal information. This information included clients' names, addresses, social security numbers, and in some cases, financial account/routing numbers. The data did not include online account credentials. It appears that as a result of this breach, the information was then used to file fraudulent tax returns with the IRS. A total of four (4) Maryland residents are being notified. HWT has taken a number of steps to restore the integrity of the system, including hiring both an outside IT consultant to immediately remediate the situation and a cyber-forensic investigator to determine the nature and scope of the intrusion. These actions resulted in the identification and removal of all malware. In addition, a number of steps were taken to further safeguard clients' information going forward. Any questions can be forwarded to my attention, at the email address or phone number below.

Best,

James Vinocur, Esq. | Partner

711 3rd Avenue, Suite 1900 | New York, NY 10017-4013

DIRECT 646.292.8719 | **EXT** 8719 | **FAX** 646.292.8701 | **MOBILE** 917.612.5264

jvinocur@goldbergsegalla.com | [Biography](#)

goldbergsegalla.com



California | Connecticut | Florida | Illinois | Maryland | Missouri
New Jersey | New York | North Carolina | Pennsylvania

Privileged attorney-client communication / attorney's work product. This email message and any attachments are confidential. If you are not the intended recipient, please immediately reply to the sender and delete the message from your email system.

Horner, Wible & Terek, PC
P.O. Box 3923
Syracuse, NY 13220



Barbara A. Terek, CPA
Matthew D. Horner, CPA
Robert K. Bulloch, CPA

HORNER, WIBLE & TEREK, PC
CERTIFIED PUBLIC ACCOUNTANTS

500 Rugh Street, Greensburg, PA 15601
724-837-7141, 724-837-7172 Fax
hwt@hwtcpa.com



May 20, 2022

Re: Notice of a Data Security Incident

Please read this letter in its entirety.

Dear Parent or Guardian of [REDACTED]

We are writing to notify you that we have reason to believe that an unauthorized third party accessed a computer system that contained your personal information. We value your business and respect the privacy of your information. As a result, we would like to provide you with one year of complimentary credit and fraud monitoring services, as well as identity theft insurance at no cost. Enrollment instructions are provided with this letter.

What Happened

On or around February 15, 2022, we were informed by the IRS that a number of tax returns had been denied because they had already been filed. As a result, we engaged both an IT consultant and a cybersecurity forensic examiner to perform a thorough investigation of our network. The results of the investigation, which we obtained on May 10, 2022, indicate that an unauthorized individual installed malware on a computer that contained your personal information. We are therefore taking appropriate precautionary measures to ensure your financial security and to help alleviate any concerns you may have.

What Information Was Involved

The affected data included personal information, including names, addresses, dates of birth, and social security numbers. If you requested direct deposit for refunds or electronic funds withdrawal for payments, your bank routing and account numbers were in our system and we advise contacting your financial institution. The data did not include financial account usernames and/or passwords.

What We Are Doing

We have made immediate security changes to our computer network to further safeguard your information, including the implementation of numerous additional safeguards. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that appropriate security protocols are in place going forward. We have also informed federal law enforcement of the breach and will cooperate in any investigation. We are committed to helping those people who may have been impacted by this unfortunate situation.

* Services marked with an "*" require an internet connection and e-mail account and will require enrollment by parent or guardian first. 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.

In addition, we are providing the parents of impacted minor dependents with access to **Cyber Monitoring*** services for you and your minor child for twelve (12) months at no charge. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

To enroll in Cyber Monitoring* services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: **I3261kxmiox09** Once you have enrolled, you will click on '**Child Monitoring**' and enter the information for the child that you are wanting to be included in the monitoring. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Cyberscout representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the Cyberscout help line **1-800-405-6108** and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

What You Can Do

If you choose not to use these services, **we are strongly urging all parents to contact the credit bureaus and ensure that no credit file exists in the name of your minor child.**

If you choose to check the existence of a credit file for your minor child on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself and your child. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft and <https://www.consumer.ftc.gov/articles/how-protect-your-child-identity-theft>.

* Services marked with an "*" require an internet connection and e-mail account and will require enrollment by parent or guardian first. 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.

For More Information

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with us regarding this incident. If so, please call us at (724) 837-7141 from 9am to 5pm, Eastern Time, Monday through Friday.

We take the responsibility to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Horner, Wible & Terek, PC

Horner, Wible & Terek, PC

Horner, Wible & Terek, PC
P.O. Box 3923
Syracuse, NY 13220



Barbara A. Terek, CPA
Matthew D. Horner, CPA
Robert K. Bulloch, CPA

HORNER, WIBLE & TEREK, PC
CERTIFIED PUBLIC ACCOUNTANTS

500 Rugh Street, Greensburg, PA 15601
724-837-7141, 724-837-7172 Fax
hwt@hwtcpa.com

May 20, 2022

Re: Notice of a Data Security Incident

Please read this letter in its entirety.

We are writing to notify you that we have reason to believe that an unauthorized third party accessed a computer system that contained your personal information. We value your business and respect the privacy of your information. As a result, we would like to provide you with one year of complimentary credit and fraud monitoring services, as well as identity theft insurance at no cost. Enrollment instructions are provided with this letter.

What Happened

On or around February 15, 2022, we were informed by the IRS that a number of tax returns had been denied because they had already been filed. As a result, we engaged both an IT consultant and a cybersecurity forensic examiner to perform a thorough investigation of our network. The results of the investigation, which we obtained on May 10, 2022, indicate that an unauthorized individual installed malware on a computer that contained your personal information. We are therefore taking appropriate precautionary measures to ensure your financial security and to help alleviate any concerns you may have.

What Information Was Involved

The affected data included personal information, including names, addresses, dates of birth, and social security numbers. If you requested direct deposit for refunds or electronic funds withdrawal for payments, your bank routing and account numbers were in our system and we advise contacting your financial institution. The data did not include financial account usernames and/or passwords.

What We Are Doing

We have made immediate security changes to our computer network to further safeguard your information, including the implementation of numerous additional safeguards. Additionally, we have engaged appropriate experts to assist us in conducting a full review of our security practices and systems to ensure that appropriate security protocols are in place going forward. We have also informed federal law enforcement of the breach and will cooperate in any investigation. We are committed to helping those people who may have been impacted by this unfortunate situation.

* Services marked with an "*" require 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.

In addition, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring*** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. 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, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. **When prompted please provide the following unique code to receive services: l31neumuxnvj** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line **1-800-405-6108** and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

What You Can Do

You are encouraged to remain vigilant against fraud and identity theft, including over the next twelve to twenty-four months, by regularly reviewing financial account statements and monitoring credit reports for suspicious activity, and to immediately report any unauthorized charges to the card issuer. The phone number to call is usually on the back of the credit or debit card. Any incidents of suspected identity theft may be reported to financial institutions and law enforcement, including the Federal Trade Commission. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report at the numbers and websites identified below.

You also have the right to place a “security freeze” on your credit report at no cost or charge, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who may access 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 to lift a security freeze on your credit report. Should you wish to place a security freeze, or to obtain a free copy of your credit report, please contact the major consumer reporting agencies.

* Services marked with an “*” require 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.

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, I recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Horner, Wible & Terek, PC

As an alternative to a security freeze, you have the right to place a “fraud alert” on your 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 agencies. You may also contact the Federal Trade Commission for additional information regarding consumer protection at:

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Ave., NW
Washington, DC 20580
Toll-Free: (877) 438-4338
TTY: 1-866-653-4261

<https://www.identitytheft.gov>

<http://ftc.gov/idtheft>

<https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services>

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

You have the right to file or obtain a police report. If you suspect you have been the victim of identity theft, you are advised to report suspected identity theft to local law enforcement, including your state Attorney General and the Federal Trade Commission.

* Services marked with an “*” require 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.

For More Information

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with us regarding this incident. If so, please call us at (724) 837-7141 from 9am to 5pm, Eastern Time, Monday through Friday.

We take the responsibility to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Horner, Wible & Terek, PC

Horner, Wible & Terek, PC

Additional Important Information

For residents of Maryland: Residents of Maryland are advised that the toll-free number for the Maryland Attorney General is 1-888-743-0023, the address is 200 Saint Paul Place, Baltimore, MD, 21202, and the website is <https://www.marylandattorneygeneral.gov/>. Individuals can obtain information from the Maryland Attorney General on how to avoid identity theft.

* Services marked with an “*” require 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.