BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

August 7, 2024

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Brown:

We are writing on behalf of our client, Heier Weisbrot & Bernstein, LLC to notify your office of a cybersecurity incident that involved 39 Maryland residents' information. Heier Weisbrot & Bernstein, LLC is headquartered in Gibbsboro, New Jersey.

Heier Weisbrot & Bernstein, LLC recently completed its investigation of an incident involving unauthorized access to a certain computer system in its network. On June 27, 2024, Heier Weisbrot & Bernstein, LLC detected an attempt by an unauthorized actor to file fraudulent tax returns for a small number of clients. The fraudulent returns were identified and reported to the IRS to be remedied. Heier Weisbrot & Bernstein, LLC worked with the IRS to ensure that any other attempted fraudulent returns are not processed.

Heier Weisbrot & Bernstein, LLC launched an investigation with the assistance of a third-party cybersecurity firm. The investigation found that an unauthorized actor accessed Heier Weisbrot & Bernstein, LLC's tax software between approximately June 22 and June 26, 2024. The files accessible in the tax software contained the name and one or more of the following for 39 Maryland residents: Social Security number, driver's license number, and financial account number(s) used for direct deposit of any tax refund if provided to Heier Weisbrot & Bernstein, LLC. For certain of the individuals, the investigation could not conclusively determine whether any of their information was accessed or acquired by the unauthorized actor. Heier Weisbrot & Bernstein, LLC completed its analysis of the personal information contained in its tax software on July 29, 2024.

On August 7, 2024, Heier Weisbrot & Bernstein, LLC commenced mailing notifications to the Maryland residents via U.S. First-Class mail in accordance with Md. Code Ann., Com. Law § 14-3504.[1] A copy of the notification is enclosed. Heier Weisbrot & Bernstein, LLC is offering complimentary credit monitoring, fraud consultation, and identity theft restoration services through IDX to all of these Maryland residents.

To reduce the risk of a similar incident from occurring in the future, Heier Weisbrot & Bernstein, LLC has and will continue to take steps to enhance the security of its computer systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Patrick H. Haggerty
Partner

Enclosure

[1] This report does not waive Heier Weisbrot & Bernstein, LLC's objection that Maryland lacks regulatory authority over it related to any claims that may arise from this incident.

HEIER WEISBROT & BERNSTEIN, LLC
CERTIFIED PUBLIC ACCOUNTANTS

Return Mail to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>
To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

August 7, 2024

Dear <<First Name>> <<Last Name>>,

Heier Weisbrot & Bernstein, LLC is writing to notify you of a data security incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and some additional steps you may consider taking in response.

We recently completed the investigation of an incident involving unauthorized access to a certain computer system in our network and an attempt by an unauthorized actor to file fraudulent tax returns for a small number of our clients through our tax software that we detected on June 27, 2024. Those fraudulent returns were identified and reported to the IRS to be remedied. We worked with the IRS to ensure that any other attempted fraudulent returns are not processed.

We also launched an investigation with the assistance of a third-party cybersecurity firm. The investigation found that an unauthorized actor accessed our tax software between approximately June 22 and June 26, 2024. The files accessible in our tax software contained your name, Social Security number, driver's license number, and financial account number(s) used for direct deposit of any tax refund if provided to us.

While we have not been able to conclusively determine whether your information was accessed or acquired by the unauthorized actor, we are offering you one year of complimentary identity monitoring services through IDX. IDX identity protection services include: one year of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-888-764-1577 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. Please note the deadline to enroll is November 7, 2024. For more information on identity theft prevention, please see the pages following this letter.

We strongly encourage you to enroll in the IRS' Identity Protection PIN ("IP PIN") program. Once you enroll, the IRS will issue you a unique PIN that helps prevent anyone from using your Social Security number to file a fraudulent tax return in the future. Please visit IRS.gov/IPPIN to get your IP PIN.

We apologize for any inconvenience this may have caused. We have and will continue to take steps to enhance the security of our computer systems to help prevent events such as this from occurring in the future.

If you have any questions about this incident, please call 1-888-764-1577, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Heier Weisbrot & Bernstein, LLC

Steps to Help Protect Your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-764-1577 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft while your IDX identity protection membership is active, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12–24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

> *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
> *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
> *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

> *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That is because most creditors need to see your credit report before they approve a new account. If they cannot see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

> **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
> **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
> **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com

You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Heier Weisbrot & Bernstein, LLC is located at 200 Haddonfield Berlin Road Suite 402, Gibbsboro, NJ 08026, and can be reached by phone at (856) 673-1929.

Additional Information for Residents of the Following States

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, https://www.marylandattorneygeneral.gov/

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.