

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite
3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

December 12, 2024

Via Electronic Mail

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown,

We represent Wonder CPA Firm PC (“Wonder CPA”) with respect to a data security incident involving personal information described below. Wonder CPA takes the security of the information in its control seriously and is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On July 1, 2024, Wonder CPA discovered suspicious activity on its systems, immediately implemented its incident response protocols, and began an internal investigation. Wonder CPA also engaged external computer forensic specialists to assist with determining what occurred and whether any data was at risk. The investigation identified unauthorized access to Wonder CPA systems. Wonder CPA reviewed the information present on its systems to identify any personal information. This review was completed on November 25, 2024, at which point Wonder CPA determined that potentially impacted information included name, address, date of birth, and Social Security number. Wonder CPA is not aware of any misuse of any information.

2. Number of residents affected.

Thirteen (13) Maryland residents were notified of the incident. A notification letter was sent to the potentially affected individuals on December 12, 2024. A copy of the form notification letter is enclosed as Exhibit A.

3. Steps taken in response to the incident.

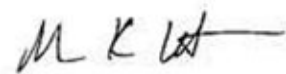
Since the incident, Wonder CPA has deployed enhanced endpoint monitoring software, performed global password reset, and implemented additional security controls. Additionally, letters were mailed to potentially affected individuals, which included instructions for enrolling in 12 months of credit monitoring and identity protection services through Cyberscout at no cost.

4. Contact Information

Wonder CPA takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

A handwritten signature in dark ink, appearing to read "M K Ventrone", with a horizontal line extending to the right.

Melissa K. Ventrone
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com



0000775

Wonder CPA Firm-W2
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB09273B

4_0000775



[REDACTED]
[REDACTED]
[REDACTED]



December 12, 2024

Notice of Data Breach

Dear [REDACTED]:

We wanted to let you know about a data security incident that may have impacted your personal information. Wonder CPA Firm PC ("Wonder CPA") may have your information if you or a business you worked for obtained tax or accounting services from us. We may also have your information if we provided payroll services to a current or former employer. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On July 1, 2024, we discovered suspicious activity on our systems. We immediately implemented our incident response protocols and began an internal investigation. External computer forensic specialists were engaged to help us determine what had occurred, and whether any information was at risk. The forensic investigation found that some documents were taken from our network. We reviewed these documents and on October 16, 2024, determined that some of your personal information was present. While we are not aware of any misuse of your information, we wanted to inform you of this incident and provide you with resources to protect your information.

What Information Was Involved?

Potentially impacted information may include your name, address, and date of birth and Social Security number.

What We Are Doing:

We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software, performed global password reset, and implemented additional security controls.

In addition, we are providing you with 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 twelve (12) months 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, a TransUnion company, specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

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.

What You Can Do:

It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact Cyberscout with any questions and to enroll in the free identity protection services. Please note the deadline to enroll is March 12, 2025. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information:

If you have any questions or concerns, please call 1-833-799-4376, Monday through Friday from 8 am - 8 pm Eastern Time, excluding holidays. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you

Sincerely,

Steven Wonder

Wonder CPA Firm PC



Recommended Steps To Help Protect Your Information

1. Website and Enrollment. Go to <https://bfs.cyberscout.com/activate> 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 Cyberscouts 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, Cyberscout will be able to assist you.

3. Telephone. Contact TransUnion at 1-833-799-4376 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 twelve (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 Transunion identity protection, notify them immediately by calling or by logging into the COMPANY 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 our 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 as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Credit Bureaus:

Equifax Fraud Reporting
P.O. Box 105788
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and
Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 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 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 a 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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.



Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. Total Rhode Island residents notified is 3.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

