



Paul F. Schmeltzer
T (213) 417-5163
F +121348811
Email:pschmeltzer@ClarkHill.com



August 9, 2022

Via USPS

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

We represent Sam Goldstein CPA ("Goldstein CPA") with respect to a data security incident involving the potential exposure of personally identifiable information described in more detail below. Goldstein CPA takes the security of information in its control seriously and has taken steps to prevent a similar incident in the future.

1. Nature of security incident.

On April 20, 2022, an employee of Goldstein CPA was unable to access their corporate email account. Goldstein CPA reset the password on the employee's email account and engaged an independent computer forensic firm to assist in responding to and investigating this incident. The forensic investigation determined that Goldstein CPA's MS365 environment showed possible indicators of compromise to the employee's corporate email account. On July 26, 2022, the investigation found that personal information was stored in the files in the impacted email account. Information present in the email account could have included some combination of name, driver's license number, passport number, mailing address, and Social Security number.

2. Number of residents affected.

Two (2) Maryland residents were notified of the incident. A notification letter was sent to the affected individuals on August 10, 2022 via regular mail. A copy of the form notification letter is enclosed.

3. Steps taken relating to the incident.

In response to the incident, Goldstein CPA implemented a password change to the impacted Goldstein CPA email account. Independent computer forensic experts were engaged to assist with determining the scope and impact of the incident, and the Goldstein CPA employee's computer

August 9, 2022
Page 2

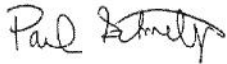
was replaced. Impacted individuals were also offered 12/24 months of credit monitoring and identity protection services through Transunion.

4. Contact Information.

Goldstein CPA remains dedicated to protecting the confidential information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at pschmeltzer@clarkhill.com or (323) 497-4493.

Very truly yours,

CLARK HILL

A handwritten signature in black ink, appearing to read "Paul Schmeltzer", with a stylized flourish at the end.

Paul F. Schmeltzer

Enclosure

Sam Goldstein, CPA, CFP
P.O. Box 3923
Syracuse, NY 13220

August 10, 2022

Notice of Data Security Incident

Dear,

We wanted to let you know about a recent data security incident experienced by Sam Goldstein CPA ("Goldstein CPA") that may have impacted your personal information. 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 April 20, 2022, an employee of Goldstein CPA was unable to access their corporate email account. After resetting the employee's email password, Goldstein CPA engaged an independent computer forensic firm to assist in responding to and investigating this incident. The forensic investigation found that Goldstein CPA's MS365 environment showed possible indicators of compromise to one account. Based on our investigation, we determined on July 26, 2022 that some of your information was present in the files in the impacted account.

What information was involved?

Information present in the email account could have included some combination of the following: your name, driver's license number, passport number, mailing address, and Social Security number.

What we are doing:

We want to assure you that we are taking steps to minimize the risk of this kind of event from happening in the future. In response to the incident, we implemented a password change to the impacted Goldstein CPA email account. Independent computer forensic experts were engaged to assist with determining the scope and impact of the incident, and the Goldstein CPA employee's computer was replaced.

Although we do not believe there is any risk that your information will be misused, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

* 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.

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 can you do:

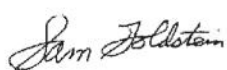
To enroll in Credit Monitoring* services at no charge, please log on to <https://secure.identityforce.com/benefit/samgoldstein> and follow the instructions provided. When prompted please provide the following unique code to receive services: **2722ABA9WJ** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

We encourage you to remain vigilant against incidents of identity theft by reviewing your bank account and other financial statements as well as your credit reports for suspicious activity for the next 12 to 24 months. You should also contact Cyberscout with any questions and to take advantage of the Cyberscout service offering. Please note you must enroll within 90 days from the date of 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

Please call 1-800-405-6108 Monday through Friday from 8:00 am to 8:00 pm Eastern Time for assistance or for any additional questions you may have. The privacy and security of your information is of the utmost importance to us, and we sincerely apologize for any inconvenience this may cause you.

Sincerely,

 *Sam Goldstein* CPA CFP

Sam Goldstein CPA

* 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.

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

You've been provided with access to the following services from Cyberscout:

- 1. Single Bureau Credit Monitoring.** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Cyberscout fraud specialist, who can help you determine if it's an indicator of identity theft.
- 2. Fraud Consultation.** You have unlimited access to consultation with a Cyberscout specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- 3. Identity Theft Restoration.** If you become a victim of identity theft, an experienced Cyberscout licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.
- 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.

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:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

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

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

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.

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

* 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.

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.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.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/201904_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: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There were 0 Rhode Island residents impacted by this incident.

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

* 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.