

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

Clark Hill LLP
555 South Flower Street, 24th Floor
Los Angeles, CA 90071
T (213) 891-9100
F +12134881178

December 21, 2023

Via Electronic Mail to IDTheft@oag.state.md.us

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

Dear Attorney General Anthony Brown:

We represent AGY Holding Corp. (“AGY”) with respect to a data security incident involving the potential exposure of limited personally identifiable information (“PII”) described in more detail below. AGY is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On November 3, 2023, AGY identified suspicious activity on a limited number of servers. AGY began an internal investigation and determined that they had suffered a ransomware attack. They immediately implemented their incident response protocols and engaged an independent computer forensic firm to assist in responding to and investigating this incident. The investigation found that a limited amount of personal information was stored on one of the affected servers, but was unable to determine whether the information was compromised. The potentially impacted information could include names, addresses, dates of birth, and Social Security numbers.

2. Number of residents affected.

Two (2) Maryland residents may have been affected and were notified of the incident. A notification letter was sent to potentially affected individuals on December 21, 2023 (a copy of the template letter is enclosed as Exhibit A).

3. Steps taken or plan to take relating to the incident.

AGY has taken steps to minimize the risk of this kind of event from happening in the future. In response to the incident, access to certain servers within the environment were temporarily disconnected and endpoint protection software was deployed on all systems. Independent

December 21, 2023

Page 2

computer forensic experts were engaged to assist with determining the scope and impact of the incident.

In addition, the potentially impacted individuals can enroll in 24 months of complimentary credit monitoring and identity restoration services provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

4. Contact information.

AGY takes the security of information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at pschmeltzer@clarkhill.com or (323) 497-4493.

Sincerely,

CLARK HILL

A handwritten signature in dark ink, appearing to read "Paul Schmeltzer", is positioned above a horizontal line.

Paul F. Schmeltzer
Attorney

CC: Melissa Ventrone, Clark Hill, PLC

Enclosure

AGY Corporation
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB08282 1-1



[REDACTED]
[REDACTED]
[REDACTED]



December 21, 2023

Notice of Data Security Incident

Dear [REDACTED],

We wanted to let you know about a recent data security incident that may have impacted your personal information. AGY Holding Corp. (“AGY”) takes the privacy and security of your information seriously, and sincerely apologizes 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 November 3, 2023, AGY identified suspicious activity on a limited number of servers. We began an internal investigation and determined that we had suffered a ransomware attack. We immediately implemented our incident response protocols and engaged an independent computer forensic firm to assist in responding to and investigating this incident. The investigation found that your personal information was stored on one of the affected servers but was unable to determine whether your information was compromised. We wanted to let you know about this incident out of an abundance of caution.

What Information Was Involved?

Information stored in our system may include some combination of your name, address, date of birth, 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, access to certain servers within the environment were temporarily disconnected and endpoint protection software was deployed on all systems. Independent computer forensic experts were engaged to assist with determining the scope and impact of the incident.

Although we have no evidence your information has been misused, we arranged for you to receive Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 24 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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

For more information:

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 1-833-961-5230 and supply the fraud specialist with your unique code listed below. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

AGY Holding Corp.

Recommended Steps to Help Protect your Information

1. Website and Enrollment. To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/agycorp> and follow the instructions provided. When prompted please provide the following unique code to receive services: **QS925TX8BE**. 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.

2. Activate the credit monitoring provided as part of your services with Cyberscout. The monitoring included 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 provide guidance.

3. Telephone. Contact Cyberscout at 1-800-405-6108 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 Cyberscout credit monitoring, notify them immediately by calling 1-800-405-6108 from 8:00 am to 8:00 pm Eastern, Monday through Friday.

A representative 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 able to work with a representative who will assist you with resolving any fraudulent activity.

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.

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.

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 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.

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.