

WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

7 ST. PAUL STREET
BALTIMORE, MD 21202-1636
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

October 29, 2021

Privileged and Confidential
VIA EMAIL (doj-cpb@doj.nh.gov)

Hon. John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Security Breach Notification

Dear Attorney General Formella,

We are writing on behalf of our client, AGI Publishing, Inc. (d/b/a Valley Yellow Pages) (“AGI”) (located at 1850 N Gateway Blvd, Fresno, CA 93727) to notify you of a data security incident involving two (2) New Hampshire residents.¹

Nature

On September 11, 2021, AGI discovered that they were the victim of a sophisticated ransomware attack that resulted in encryption and unauthorized access to their network. At that time, AGI took immediate steps to stop the threat and understand the full scope of the situation. This included hiring third-party forensic experts to conduct a thorough investigation, remediation efforts, and contacting the FBI to seek assistance with the incident. On October 19, 2021, AGI concluded its initial investigation and found that the unauthorized individual(s) gained access to its systems via a VPN access, which has been remedied and secured.

Concurrently, AGI began a comprehensive search of the data to determine what information was involved and the individuals the incident impacted. AGI recently concluded its review and determined that the incident involved personal information related to two (2) New Hampshire residents.

The personal information that was potentially impacted included social security numbers and the protected health information that was potentially impacted included first and last names, addresses, health/dental plan numbers, and premium amounts paid.

¹ By providing this notice, AGI does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Notice and AGI's Response to the Event

On October 29, 2021, AGI will mail a written notification to the potentially affected New Hampshire residents, pursuant to N.H. Rev. State § 359-C:19, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, AGI is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through Experian;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and
- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, AGI provided the notice to the three major credit reporting agencies along with the applicable government regulators, officials, and other Attorneys General (as necessary).

Finally, AGI is working to implement any necessary additional safeguards, enhance and improve its policies and procedures related to data protection, improve its cybersecurity infrastructure, and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,

A handwritten signature in blue ink, appearing to read "Spencer S. Pollock".

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A



The better book...

AGI Publishing Inc.
1850 N. Gateway Blvd.
Fresno, CA 93737

October 29, 2021

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

H0134-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 CA



APT ABC
123 ANY STREET
ANYTOWN, FC
COUNTRY



Re: Notice of Data Breach

Dear Sample A. Sample:

At AGI Publishing, Inc. (d/b/a Valley Yellow Pages) (“AGI”) we value transparency and respect the privacy of your information, which is why we are writing to let you know about a data breach that may involve your personal information, what we did in response, and steps you can take to protect yourself against possible misuse of your personal information.

What Happened

On September 11, 2021, we discovered that we were the victim of a sophisticated ransomware attack that impacted our networks and servers. After discovering the incident, we quickly took steps to secure and safely restore our systems and operations via viable backups. Further, we immediately engaged outside counsel and third-party forensic experts to conduct a thorough investigation of the incident's nature and scope, assist in remediation efforts, and contacted and filed a report with the FBI. We concluded our investigation on October 19, 2021, and determined that the unauthorized individual gained access to and potentially obtained information from our systems.

Concurrent to our investigation, we began a comprehensive review of the impacted data and believe that your personal and/or protected health information was potentially involved in the incident. *However, as of now, we have no evidence indicating misuse of any information, but we wanted to notify you of this incident out of an abundance of caution.*

What Information Was Involved

The types of information potentially involved are your first and last name, address, social security number and date of birth. If you were on the health plan between 2016 and 2018, the impacted information may also include your health plan number and monthly premium amount. If you were on the Ameritas dental plan any time since 2007, the impacted information may also include your payment amounts for dental claims.

What We Are Doing

As explained above, we took immediate steps to secure our systems, contacted the FBI, and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we are implementing additional cybersecurity safeguards, enhancing our employee cybersecurity training, and working to improve our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident from occurring again.

0000001



What You Can Do

The security and privacy of the information contained within our systems is a top priority for us. Therefore, while we have no evidence indicating your information was misused, we strongly recommend you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement. Please see “***Other Important Information***” (attached) for guidance on how to best protect your identity.

To help protect your identity, we are offering a complimentary 12-month membership of Experian’s® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: January 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian’s customer care team at (833) 210-4611 by **January 31, 2022**. Be prepared to provide engagement number **B020768** as proof of eligibility for the identity restoration services by Experian. Please see the next page for additional information about these services.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have any additional questions, please call our toll-free response line at (833) 210-4611 between Monday through Friday from 6 a.m. to 8 p.m. Pacific, and Saturday and Sunday from 8 a.m. to 5 p.m. Pacific.

Sincerely yours,

Jason Hamm, General Counsel

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 210-4611. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12-months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax
(888) 766-0008
P.O. Box 740256
Atlanta, GA 30374
www.equifax.com

Experian
(888) 397-3742
P.O. Box 2104
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
P.O. Box 6790
Fullerton, CA 92834
www.transunion.com

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

| | | |
|---|---|--|
| Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/ | Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze | TransUnion Security Freeze & Fraud Victim Assistance Dept. P.O. Box 6790 Fullerton, CA 92834 https://www.transunion.com/credit-freeze |
|---|---|--|

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity.

As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf/0009_identitytheft_a_recovery_plan.pdf.

District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov. **Iowa residents** may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa*, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319. **Maryland residents** may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **Massachusetts residents:** State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **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. **New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, <https://ag.ny.gov/internet/resource-center> and or *NYS Department of State's Division of Consumer Protection*, (800) 697-1220, <https://www.dos.ny.gov/consumerprotection>. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office, Consumer Protection Division*, 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents:** State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents.** There were 582 Rhode Island residents potentially impacted. You have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West**



Virginia residents have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.