

October 24, 2022

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attorney General Brian E. Frosh
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Data Incident Notification

Dear Attorney General Frosh:

APG Media Group of Southern Wisconsin, LLC (“APG”), owner/operator of the Janesville Gazette. APG hereby formally submits notification of a recent data incident pursuant to Md. Code Ann. Comm. Law 14-3504. APG reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, APG does not waive any rights or defenses regarding the applicability of Maryland law, including the applicability of Md. Code Ann. Law 14-3504, the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over APG.

On June 7, 2022, APG became aware that an unauthorized third party had gained access to some of the Janesville Gazette’s systems and servers on May 25, 2022 (the “Incident”). APG discovered the Incident when an employee discovered ransom notes being automatically printed. Immediately upon learning of the Incident, APG isolated the impacted environment and began an investigation with the help of a leading forensic security firm that specializes in data security and ransomware incidents. As part of its investigation, APG also worked with third-party data mining experts to identify who was impacted by this Incident. These experts analyzed the impacted data to determine what personal information may have been accessed. After securing its systems, reviewing the results of the investigation, and assessing what information was impacted, APG determined on September 22, 2022, that personal information of former and current employees and some dependents were accessed and/or acquired by the third party during the Incident. At this time, APG does not have any evidence that any fraud or identity theft has occurred as a result of this Incident. In light of the foregoing and out of an abundance of caution, APG has decided to notify your office (via this letter) and the one (1) Maryland resident potentially affected by this Incident via U.S. Mail on or about October 25, 2022. A sample notification letter to the affected resident is attached hereto as Exhibit A.

APG takes the security of personal information seriously. APG has taken further steps to bolster the security of its networks and systems, including by strengthening its security tools to

Attorney General Brian E. Frosh

October 24, 2022

Page 2

include a more sophisticated endpoint detection software. In addition, APG has retained IBC to provide notice to affected individuals and Experian to provide free identity theft and credit monitoring services.

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

Sincerely,

GODFREY & KAHN, S.C.

A handwritten signature in black ink, appearing to read 'Sarah A. Sargent', written in a cursive style.

Sarah A. Sargent

SAS:cg

EXHIBIT A

Sample Notification Letter



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741



October 25, 2022

Notice of Data Breach

Dear [REDACTED]:

At APG Media Group of Southern Wisconsin, LLC (APG), owner/operator of the Janesville Gazette, we take your privacy seriously. For that reason, we are writing to provide you with notice of a recent cybersecurity event that involved your personal information. You are receiving this notice because you either are or were an employee of APG and/or Bliss Communications or were listed as a dependent of an APG and/or Bliss Communications employee. Consistent with our commitment to protect the information of our current and former employees and their dependents, we have investigated the incident and, as a precautionary measure, we are notifying you of the event and the additional protections that are available to you listed below.

What Happened

On June 7, 2022, APG became aware that an unauthorized third party had gained access to some of the Janesville Gazette's systems and servers on May 25, 2022. Immediately upon learning of the incident, APG isolated the impacted environment and began an investigation with the help of a leading forensic security firm that specializes in data security and ransomware incidents. As part of our investigation, APG also worked with third-party data mining experts to identify who was impacted by this incident. These experts analyzed the impacted data to determine what personal information may have been accessed. After the investigation, it was determined that your personal information was accessed and/or acquired by the third party during the incident. While APG does not have any evidence of fraud using your personal information at this time, we are nonetheless informing you of this incident because we take this matter seriously. While APG did notify law enforcement of this incident, this notice was not delayed at the request of law enforcement.

What Information Was Involved

Your personal information that was impacted includes your name and the following: [REDACTED]

What We Are Doing

Upon discovery of the incident, APG immediately took steps to re-assess the security of our systems to mitigate the impact of the event. In addition to fully investigating this incident and providing notice to you through this letter, we have taken additional actions to improve and monitor the security of our systems, including strengthening our security tools to include a more sophisticated endpoint detection software.

Additionally, 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: 1/14/2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code** [REDACTED]

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 **1-877-288-8057** by **1/14/2023**. Be prepared to provide engagement number **B079337** as proof of eligibility for the identity restoration services by Experian. For more information regarding IdentityWorks, please see the enclosed information.

What You Can Do

We encourage you to contact Experian with any questions and to enroll in the free identity protection services. In addition, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, 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. We encourage you to take full advantage of this service offering.

For More Information

We sincerely apologize for this incident and regret any inconvenience it may cause you. If you have questions, please call (866) 877-4420, Monday through Friday from 9:00 am - 7:00 pm EST.

Sincerely,



David Alltop
VP of IT
APG Media Group of Southern Wisconsin, LLC

ADAMS-ADT

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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists 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 877.288.8057. 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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report: It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts: There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze: You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices: 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, the Attorney General's office in your home state, or your local law enforcement. In certain states you have the right to obtain a police report if you are a victim of identity theft. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Fair Credit Reporting Act: You have certain rights pursuant to the Fair Credit Reporting Act. If you would like additional information regarding your rights under the Fair Credit Reporting Act, you can review your rights by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 or 919-716-6000.

For 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/>. You can also contact the 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/>;

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.