Donna Maddux
4800 SW Meadows Road
Suite 300
Lake Oswego, Oregon 97035
Mobile: 503.312.6251
Email: dmaddux@constangy.com

January 25, 2023

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall St., 6th Floor
Augusta, ME 04330

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith, and Prophete LLP represents Andrews McMeel Universal ("AMU") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in compliance with Maine's data breach notification statute.

1. **Nature of the Security Incident**

On November 19, 2022, AMU experienced a network disruption. AMU immediately took steps to secure the network environment. AMU also engaged cybersecurity experts to assist with safely restoring operations, to investigate the incident, and to determine if any personal information was impacted. The investigation determined that an unknown actor gained access to and obtained certain data from the AMU network. On January 4, 2023, we determined that certain personal information was involved.

Please note that to date, there is no reason to believe that personal information of impacted individuals has been misused as a result of this incident.

2. **Number of Affected Maine Residents Impacted & Information Involved**

On January 25, 2023, AMU notified five (5) Maine residents by letter mailed via first class U.S. mail. A sample copy of the notification letter is included with this correspondence.

The impacted information varies by individual, but may include the residents' Social Security numbers, dates of birth, financial account information, driver's licenses, passport numbers, health insurance information, and/or medical information.

This round of notification includes current and past employees and 1099 contractors with available address information. AMU is in the process of conducting a review of the impacted data set, and an additional round of notification may be forthcoming at the conclusion of data mining.

3. **Measures Taken to Address the Incident**

In response to the incident, AMU retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. AMU implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. AMU also reported this incident to federal law enforcement and is cooperating with the investigation.

AMU is notifying the affected individuals and providing resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose personal information was affected by this event, including credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered through IDX. IDX will also support a call center for 90 days to answer questions and assist with enrollment.

Finally, AMU is reporting this incident out of an abundance of caution to the three credit reporting agencies: Experian, Equifax, and TransUnion.

4. **Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at DMaddux@constangy.com or 503.312.6251.

Sincerely,

Donna Maddux of
Constangy, Brooks, Smith, and Prophete LLP

Encl.: Sample Notification Letter

Andrews McMeel Universal

10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<code>>

<<first name>> <<last name>>
<<address>> <<address2>>
<<city>>, <<state>><<zip>>

January 25, 2023

Re: Notice of Data <<Security Incident/Breach>>

Dear <<first name>> <<lastname>>:

We are writing to inform you of a data security incident experienced by Andrews McMeel Universal that may have involved your personal information. At Andrews McMeel Universal, we take the privacy and security of the personal information in our possession very seriously. That is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and are offering you the opportunity to enroll in complimentary credit monitoring and identity monitoring.

What Happened? On November 19, 2022, Andrews McMeel Universal experienced a network disruption. We immediately took steps to secure the network environment. We also engaged cybersecurity experts to assist us with safely restoring our operations, to investigate the incident, and to determine if any personal information was impacted. The investigation determined that an unknown actor gained access to and obtained certain data from the Andrews McMeel Universal network. On January 4, 2023, we determined that your personal information was involved.

What Information Was Involved? The information involved may include your name, Social Security number, passport number, driver's license number, date of birth, health insurance information, and medical information.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also notified law enforcement and are cooperating with the resulting investigation. We are providing you with information about steps you can take to help protect your personal information. In addition, we are offering you complimentary identity monitoring and recovery services for <<12/24>> months through IDX as described below.

What You Can Do: We recommend that you review the guidance included with this letter about how to protect your personal information. We also encourage you to enroll in the complimentary credit monitoring and identity monitoring IDX services, which are free to you upon enrollment, include a subscription for the following: single bureau credit monitoring, CyberScan dark web monitoring, fully-managed identity recovery services, and $1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised.

To receive credit services, you must be over the age of 18, and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. Additional information describing your services is included with this letter.

Please note you must enroll by April 25, 2023. 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.

For More Information: If you have any questions about the complimentary services or need assistance, please contact customer service for IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

On behalf of Andrews McMeel Universal, please accept our sincere apologies and know that we deeply regret any concern or inconvenience this matter may cause you. We want to emphasize that we are taking this situation extremely seriously as the privacy and protection of personal information is a top priority for Andrews McMeel Universal. We have taken and continue to take steps to protect against a similar incident from occurring in the future.

Sincerely,

Alexander H. Sareyan
Chief Executive Officer
Andrews McMeel Universal

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 2000	P.O. Box 4500	P.O. Box 740256	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-888-378-4329	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.com

Fraud Alert: 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 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov; https://oag.dc.gov/

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; https://www.marylandattorneygeneral.gov/

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; https://ncdoj.gov/

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Rhode Island: The total number of individuals receiving notification of this incident is 1,267. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov; https://ago.vermont.gov/