Lowenstein Sandler

Mary J. Hildebrand
Partner

One Lowenstein Drive
Roseland, New Jersey 07068

September 8, 2023

Via Regular Mail & Email (attorneygeneral@doj.nh.gov)

Attorney General John Formella
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, New Hampshire 03301
attorneygeneral@doj.nh.gov

To Whom It May Concern:

We represent the Associated Press ("AP") in connection with a security incident that affected the personal information of two (2) New Hampshire residents.

AP Stylebook is a service offered by the AP. The affected personal information was stored in a database that was accessible on a legacy AP Stylebook website that was no longer in use but still available online and maintained on behalf of AP by an outside service provider, Stylebooks.com, Inc. ("Stylebooks.com"). As a result of the security incident described below, personal information of AP Stylebook customers stored on the legacy website was unlawfully accessed and may have been acquired by an unauthorized third party.

What Happened? On July 20, 2023, Stylebooks.com notified AP that AP Stylebook customers had received phishing emails directing them to a fake website that imitated AP Stylebook to provide updated credit card information. AP immediately engaged a cyber forensics firm to investigate the incident. The firm reported that personal information of customers whose information was stored on the old AP Stylebook website had been accessed by an unauthorized third party between July 16 and July 22, 2023, and that the phishing emails had been sent to those customers. The active AP Stylebook website (https://www.apstylebook.com) was not affected by this security incident.

What Information Was Involved? AP received the first information on the potentially affected customers on 2 August 2023. The personal information affected included the , . AP Stylebook had also requested , where applicable, when customers made a purchase, and Stylebooks.com records showed that some New Hampshire residents submitted a . Because AP cannot rule out that the provided in response to that request by New Hampshire residents is a

, AP decided to proactively let residents of New Hampshire know that their may have been accessed and acquired by third parties as a result of this incident.

What We Have Done/Are Doing. AP takes this incident and information security very seriously. AP immediately engaged with its service provider Stylebooks.com and forensic experts to carry out a full investigation and to assist it in assessing and mitigating the incident. On July 23, 2023, the legacy AP Stylebook website was taken offline, and on July 27, 2023, the fake Stylebooks website was taken down. On July 27, 2023, AP sent an email to all AP Stylebook customers (both customers that used the legacy website and customers that use the current AP Stylebook website). In this email, AP alerted the recipients to the phishing emails, clarified which email address is used to send legitimate emails, and provided its contact information for any questions. AP is also forcing all AP Stylebook customers to change their passwords prior to accessing the active AP Stylebook website. In addition to these measures, AP is reviewing its security protocols and enhancing its internal training programs.

Credit Monitoring Service. While AP is unaware of any identity theft or fraud as a result of this event, AP is offering the two (2) New Hampshire residents access to 24 months of complimentary credit monitoring and identity restoration services through Experian.

AP sent a notification to the two (2) New Hampshire residents on September 1, 2023, via regular mail. Please find attached a sample copy of such notification.

If you have any comments or questions, please contact the undersigned.

Very truly yours,

Mary J. Hildebrand

MH:lc

30400/10
9/8/23 214472700 1

«Name1» «Name2» «Name3»
«Address1»
«Address2»
«City», «State» «Zip»
«Country»

September 1, 2023

Notice of Data Breach

Dear «Name1»:

We at the Associated Press Stylebook ("APS") are contacting you to provide you with important information about a data security incident that affected your personal information. The personal information was stored in a database that was accessible on an old AP Stylebook website that was no longer in use but still available online and maintained on our behalf by an outside service provider, Stylebooks.com, Inc. ("Stylebooks.com"). As a result of the security incident described below, personal information of AP Stylebook customers stored on the old website was unlawfully accessed and may have been acquired by an unauthorized third party. Although we have no indication of identity theft or fraud in relation to this incident at this time, we are providing you with information about the incident, our response, and additional measures you can take to help protect your personal information.

What Happened? On July 20, 2023, Stylebooks.com notified us that AP Stylebook customers had received phishing emails directing them to a fake website that imitated AP Stylebook to provide updated credit card information. APS immediately engaged a cyber forensics firm to investigate the incident. The firm reported that personal information of customers whose information was stored on the old AP Stylebook website had been accessed by an unauthorized third party between July 16 and July 22, 2023, and that the phishing emails had been sent to those customers. The active AP Stylebook website (https://www.apstylebook.com) was not affected by this security incident.

What We Have Done/Are Doing. APS takes this incident and information security very seriously. We immediately engaged with our service provider Stylebooks.com and forensic experts to carry out a full investigation and to assist us in assessing and mitigating the incident. On July 23, 2023, the old AP Stylebook website was taken offline, and on July 27, 2023, the fake spoofed Stylebooks website was taken down. On July 27, 2023, we sent an email to all AP Stylebook customers (both customers that used the old website and customers that use the current AP Stylebook website). In this email, we alerted the recipients to the phishing emails, clarified which email address is used to send legitimate emails, and provided our contact information for any questions. We are also forcing all AP Stylebook customers to change their passwords prior to accessing the active AP Stylebook website. In addition to these measures, APS is reviewing its security protocols and enhancing its internal training programs.

While we are unaware of any identity theft or fraud as a result of this event, APS is offering you access to of complimentary credit monitoring and identity restoration services through Experian. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** . Your code will not work after this date.
- **Visit** the Experian IdentityWorks website to enroll at .
- Provide your **activation code**: **«ActivationCode»**.

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 by

December 31, 2023. Be prepared to provide **engagement number** as proof of eligibility for the identity restoration services by Experian.

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:

- **Daily Credit Monitoring:** Three Bureaus (Experian, Equifax and TransUnion).
- **Credit Report:** Upon Enrollment.
- **Daily Credit Reports:** Available online.
- **Product Delivery Method:** Online (email) and Offline (U.S. Mail).
- **Enrollment**: By phone or online.
- **ExtendCare™** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Blanket Identity Restoration:** Available upon notification by you to Experian.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. Underwritten 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.

Credit Freeze: You can request a credit freeze whether or not you activate this service.

If you believe that 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) 890-9332**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, an Experian Identity Restoration agent will be 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 24 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.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring your free credit reports for suspicious activity and to detect errors, and reporting any unusual activity to your financial institution. Please also review the enclosed ***Additional Resources*** page, which contains information on what you can do to help safeguard against possible misuse of your information. You can also enroll in the credit monitoring and identity restoration services that we are offering.

Sincerely,
The Associated Press Stylebook Team

Additional Resources

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. 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 law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

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 https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:	**Experian**:	**TransUnion**:
equifax.com	experian.com	transunion.com
equifax.com/personal/credit-report-services	experian.com/help	transunion.com/credit-help
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
866-349-5191	888-397-3742	888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; 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 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 violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023. You may obtain information from the Office of the Attorney General and the Federal Trade Commission about steps to take to avoid identity theft.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General. You may obtain information from the Office of the Attorney General and the Federal Trade Commission about steps to take to avoid identity theft.

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

For Georgia, Maryland, New Jersey, 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 bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos ny.gov/consumerprotection, 1-800-697-1220.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 110 South, Washington, D.C. 20001, https://www.oag.dc.gov/, 202-727-3400. You may obtain information from the Office of the Attorney General and the Federal Trade Commission about steps to take to avoid identity theft.

For Rhode Island residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, http://www riag ri.gov, (401) 274-4400. Our investigation has determined that one Rhode Island resident was affected by this incident.