



Michael Christopher, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East, Suite 1100
Los Angeles, CA 90067
mchristopher@constangy.com
Direct: 310.912.6183
Mobile: 949-322-8874

September 27, 2024

Via Email

Attorney General Anthony Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents The Washington Time, LLC (“The Washington Times”, based in Washington, D.C., 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.

1. What Happened

On July 27, 2024, The Washington Times experienced an encryption event. Upon discovering the incident, it swiftly took steps to secure its digital environment. It also engaged a digital forensics and incident response firm to conduct an investigation to determine whether any data may have been affected. The investigation revealed that certain data stored on the network may have been accessed or acquired without authorization between July 24, 2024, and July 27, 2024. The Washington Times then undertook a comprehensive review of the potentially affected data. On September 17, 2024, it determined that certain personal information was contained in the affected data. Since then, The Washington Times has been working to gather contact information necessary to provide individuals with notice of the incident.

2. Number of Maryland Residents Notified and Type of Information

On September 27, 2024, The Washington Times notified two (2) Maryland residents of this data security incident via U.S. First-Class Mail. The data sets affected by this incident included vary by individual, but included individuals’ names, Social Security numbers, and/or driver’s license numbers. A sample copy of the notification letter sent to impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

The Washington Times has implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, The Washington Times has offered notified individuals 12 months of complimentary identity protection services through Cyberscout through Identity Force, a TransUnion company.

4. Contact Information

The Washington Times remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please contact me.

Very truly yours,

A handwritten signature in blue ink, appearing to read "MC" or "Michael Christopher", written in a cursive style.

Michael Christopher
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

The Washington Times

To Enroll, Please Visit:
<https://bfs.cyberscout.com/activate>
Enrollment Code: [CODE]

<<FirstName>> <<LastName>>
<<Address1>>
<<City>>, <<State>> <<ZIP>>

September 27, 2024

Re: Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>:

We are writing to inform you of a data security incident that may have affected your personal information. At The Washington Times LLC, we take the privacy and security of your information very seriously. That is why we are notifying you of the incident, providing you with steps you can take to help protect your information, and offering you complimentary identity protection services.

What Happened. On July 27, 2024, The Washington Times experienced an encryption event. Upon discovering the incident, we swiftly took steps to secure our digital environment. We also engaged a digital forensics and incident response firm to conduct an investigation to determine whether any data may have been affected.

The investigation revealed that certain data stored on the network may have been accessed or acquired without authorization between July 24, 2024, and July 27, 2024. The Washington Times then undertook a comprehensive review of the potentially affected data. On September 17, 2024, we determined that some of your personal information was contained in the affected data. Since then, we have been working to gather contact information necessary to provide you with this notice.

What Information Was Involved. The potentially affected information may have included your name and Social Security Number <<and driver's license or state ID number>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above. We also implemented additional measures to enhance the security of our digital environment and minimize the risk of a similar incident occurring in the future. As a further precaution, we are offering you 12 months of complimentary identity protection services through Cyberscout through Identity Force, a TransUnion company. This product helps detect possible misuse of your information and provides you with identity protection support.

What You Can Do. We encourage you to review the recommendations included with this letter to help protect your information. In addition, you can enroll in the complimentary identity protection services by logging on to <https://bfs.cyberscout.com/activate> and following the instructions provided. When prompted please provide the following unique code to receive services: <<CODE HERE>>. 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. When prompted, please provide the unique code noted above to enroll in the services. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information. If you have questions or need assistance, please call <<phone number>> Monday through Friday from <<hours>> Eastern, excluding holidays.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

The Washington Times LLC
3600 New York Ave NE
Washington, DC 2002

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:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.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 one year. 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: 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 fraud alerts, security freezes, and 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

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.