



Aubrey Weaver, Partner
Cybersecurity & Data Privacy Team
1650 Market Street
Suite 3600
Philadelphia, Pennsylvania 19103
aweaver@constangy.com

July 19, 2024

ELECTRONIC MAIL

Attorney General Anthony G. Brown
Maryland Attorney General's Office
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete LLP ("Constangy") represents Findlay Land Rover Reno, Findlay Toyota Flagstaff, and Findlay Volvo (as referred to collectively herein, "Findlay") in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in compliance with Maryland's data breach notification statute.

1. Nature of Incident

On June 7, 2024, Findlay became aware of unusual activity in its network environment. As soon as it discovered this, Findlay immediately took steps to contain the activity and engaged a cybersecurity firm to investigate what happened and help it determine whether any sensitive data was affected. Findlay's investigation revealed that certain Findlay data may have been accessed or acquired without authorization in connection with the incident. Findlay thereafter undertook a review of the potentially affected data, which revealed that certain information for Findlay employees may have been involved in this incident.

The potentially affected information includes names, Social Security numbers, driver's license numbers, passport numbers, and/or other employment-related information.

2. Number of Maryland residents affected

Findlay notified three (Findlay Land Rover Reno (1); Findlay Toyota Flagstaff (1); Findlay Volvo (1)) Maryland residents of the incident via first class U.S. mail on July 19, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

As soon as Findlay discovered the incident, it took the steps described above. Findlay has also taken steps to further bolster the security of its network and reduce the likelihood of a similar incident occurring in the future. In addition, Findlay is offering affected individuals complimentary credit monitoring and identity protection services. These services include twelve (12) months of credit monitoring, identity restoration services, and identity protection insurance through Identity Force, a TransUnion company. Findlay has also provided guidance on steps individuals can take to protect their personal information.

4. Contact information

Findlay takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 215.770.4234 or aweaver@constangy.com.

Sincerely yours,

A handwritten signature in black ink, appearing to be 'Aubrey Weaver', with a stylized, cursive script.

Aubrey Weaver of
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Consumer Notification Letter

<<Custom Field 2>>
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 19, 2024

Subject Line: Notice of Data <<Custom Field 1>>

Dear << First Name>> << Last Name>>:

<<Custom Field 2>> ("Findlay") is writing to inform you of a recent incident that may have involved your personal information. Findlay is committed to maintaining the trust of our employees, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your information. Please review the following for more information about the incident, steps you can take to help protect your personal information, and an offer of complimentary credit monitoring and identity protection services.

What Happened? On June 7, 2024, Findlay became aware of unusual activity in our network environment. As soon as we discovered this, we immediately took steps to contain the activity and engaged a cybersecurity firm to investigate what happened and help us determine whether any sensitive data was affected. Our investigation revealed that certain Findlay data may have been accessed or acquired without authorization in connection with the incident. Findlay thereafter undertook a review of the potentially affected data, which revealed that certain information for Findlay employees may have been involved in this incident. As a result, we are providing notification to all employees and providing resources to assist them.

What Information Was Involved? The potentially affected information includes your name, Social Security number, driver's license number, passport number, and/or other employment-related information.

What We Are Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We notified the Federal Bureau of Investigation and will cooperate with any resulting investigation.

In addition, to help protect your identity, Findlay is also offering you the opportunity to enroll in Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for <<service length>> months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll, please go to <https://bfs.cyberscout.com/activate> and use the Enrollment Code <<Unique Code>>. Cyberscout representatives are available for 90 days from the date of this letter to assist you with questions regarding enrollment between 5:00 am to 5:00 pm Pacific Time, Monday through Friday, excluding holidays. Please note the deadline to enroll is <<deadline date>>. 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.

What You Can Do. We encourage you to enroll in the complimentary identity protection services we are offering. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information: Cyberscout Representatives are available to assist you with questions regarding this incident, between the hours of 5:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday, excluding holidays. Please call the help line at 1-833-531-2361.

We thank you for your understanding deeply regret any worry or inconvenience that this may cause.

Very truly yours,

<<Custom Field 2>>

<<Custom Field 3>>

STEPS YOU CAN TAKE TO HELP PROTECT 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 1000
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.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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
<https://www.marylandattorneygeneral.gov/>
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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>