



January 10, 2022

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

To the Office of the Attorney General:

We are writing to inform you of a recent cyber-attack incident that may have compromised the integrity of personal information relating to 2 Maryland residents.

Between April 26, 2021 and May 3, 2021, unknown malicious actors gained access to digital files of a Farmers agent. These digital files contained information about customers and consumers. The information included name, address, social security number and date of birth. In many cases, we were not able to easily identify the potentially affected individuals and their contact information without extensive investigation and additional research.

Upon discovery of this activity on May 3, 2021, the agent has taken steps to remediate this issue, including rebuilding impacted machines, confirming appropriate updates for operating systems and applications, conducting regular malware scans, and utilizing multi-factor authentication.

We are in the process of notifying all affected individuals and will be offering credit monitoring to them. Maryland residents who were affected will be notified by mail which will be sent no later than January 27, 2022. Attached are the sample notification letters.

If you have any questions, please do not hesitate to contact me at 619-746-9009 and/or gillian.vaughn@farmersinsurance.com.

Sincerely,

Gillian Vaughn
Gillian Vaughn
Privacy and Information Governance Office
Farmers Insurance

Attachment



[Date]

[First Last
Address
City,State Zip]

NOTICE OF DATA BREACH

Dear [First name]:

What Happened?

We are writing to inform you that between April 26, 2021, and May 3, 2021, agent Curt Henderson was a victim of a cyber-attack that resulted in access to select consumer information. In many cases, we were not able to easily identify the potentially affected individuals and their contact information without extensive investigation and additional research. The agent has taken steps to remediate this issue, including rebuilding impacted machines, confirming appropriate updates for operating systems and applications, conducting regular malware scans, and utilizing multi-factor authentication.

What Information Was Involved?

We believe that the malicious actors accessed or obtained certain personal information in this attack which includes your Name, Address and <<dynamic the data elements will be populated >>. We regret this happened and sincerely apologize for any inconvenience and concern this causes you. We take the obligation to safeguard personal information seriously and are alerting you so you can take steps to help protect yourself. To do so, we encourage you to take the steps that are outlined below.

What We Are Doing.

CyberScout, has been retained to help you with any questions or problems you may encounter related to this matter, including obtaining a credit report, credit monitoring and placing fraud alerts on your behalf. To assist you, we are providing you with access to Single Bureau Credit Monitoring/Triple Bureau Credit Report* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services also will be provided by CyberScout, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.cs11protect.com> or **cs11protect.com**, click the "Sign Up" button and follow the instructions to create your account.

Enter your information and the following Access Code to complete your registration: <<Access Code>>

Next, click the "Use Now" link on the Monitoring Services tile to verify your identity and activate your monitoring services.

**Please note that when signing up for the credit and fraud monitoring products, you may be asked to verify personal information for your own protection in order to confirm your identity.*

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What You Can Do.

In addition to enrolling in credit monitoring, we recommend that you take the following precautions:

Order your free credit report – You are entitled under U.S. law to one free credit report annually from each of the three national credit bureaus. To order your free credit report, visit www.annualcreditreport.com, call toll free at **877-322-8228**, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to **Annual Credit Report Requests Service, P.O. Box 105281, Atlanta, GA 30348-5281**. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report, review it carefully. Look for accounts you did not open, inquiries from creditors you did not initiate, and any inaccurate personal information, such as your home address and telephone number. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records. Even if there are no signs of fraud, you should continue to check your credit report every three months for the next year.

Place a fraud alert on your credit bureau file – A fraud alert instructs issuers of credit to use more than normal scrutiny for any request for new or additional credit. This adds a layer of protection, but it might limit your ability to obtain *instant credit* (for example, an instant credit card offered by a retail store). You can place a fraud alert by contacting one of three national consumer reporting agencies directly at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

Place a security freeze on your credit file – Since September 21, 2018, placing a freeze on your credit file is free. Visit the credit bureau links below to determine how and what information you need to provide them to place a security freeze on your credit report to prohibit a credit bureau from releasing information from your credit report without your consent. For more information on placing a security freeze on your credit reports, please visit the following credit bureaus:

- Equifax security freeze: <https://www.equifax.com/personal/credit-report-services/credit-freeze/>
- Experian security freeze: <https://www.experian.com/freeze/center.html>
- TransUnion security freeze: <https://www.transunion.com/credit-freeze>

Report suspicious activity – If your credit accounts have any suspicious activity, you may choose to report it to the following:

- The credit bureaus listed above.
- Your relevant financial institution(s).
- The local police or sheriff's office, where you can file a report of identity theft and obtain a copy of the report. You may need the report for your creditors and relevant financial institution(s).
- The Federal Trade Commission at www.Consumer.gov/idtheft - If you believe your identity has been stolen you may use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts. You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC:

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

Maryland Residents - You may also obtain additional information about preventing identity theft by visiting:

Maryland Office of the Attorney General at:
Oag.state.md.us/idtheft/index.htm, or call 1-410-528-8662
 or write to this address:

Consumer Protection Division
 Maryland Office of the Attorney General
 200 St. Paul Place, Baltimore, MD 21202

For More Information

We realize this news is troubling, and again offer our sincerest apologies for any inconvenience this may have caused. If we may be of assistance, or if you have any additional questions, please do not hesitate to call us toll free 1-866-391-6062 or contact us at PrivacyRequest.PrivacyOffice@farmersinsurance.com.

Sincerely,

Gillian Vaughn
 Gillian Vaughn
 Privacy and Information Governance Office
 Farmers Insurance®