April 28, 2021

Attorney General Wayne Stenehjem
Office of the North Dakota Attorney General
600 E. Boulevard Ave Dept. 125
Bismarck ND 58505
Email: ndag@nd.gov

To the Office of the North Dakota Attorney General:

We are writing to inform you of a recent data security incident that may have compromised the integrity of personal information relating to 1 North Dakota resident.

Between January 20, 2021 and February 12, 2021, unknown malicious actors targeted the Farmers Insurance and 21st Century Insurance automobile insurance quoting systems to obtain various individuals' personal information. While we are still investigating this, we believe the malicious actors used certain personal information already in their possession such as name, address and/or date of birth and used that information to obtain driver's license numbers.

Upon discovery of this activity on February 5, 2021, we took immediate steps to prevent access to personal information, implemented a code fix and began working to identify the potentially affected individuals. Identification of those individuals was completed on April 16, 2021.

We are in the process of notifying all affected individuals and will be offering credit monitoring to them. The North Dakota resident who was affected will be notified by mail which will be sent no later than April 30, 2021. Attached is the sample notification letter.

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

Attachments

[Date]

[First Last
Address
City,State Zip]

NOTICE OF DATA BREACH

Dear [First name]:

We are writing to inform you of a recent security incident that involved the Farmers Insurance® online automobile insurance quoting tool.

What Happened?

I am writing to let you know that between January 20, 2021 and February 12, 2021, unknown malicious actors targeted the Farmers auto quoting system to obtain various individuals' personal information. While we are still investigating this to determine exactly how this occurred, we believe your driver's license number may have been obtained. Upon discovery of this activity, we took immediate steps to prevent access to personal information and began working to identify the potentially affected individuals.

We are notifying you and any consumers who we believe were affected by this incident. However, we believe some people receiving this letter may have made valid quote requests or had someone in their household make valid quote requests on our website during the applicable time period. Therefore, if a valid quote request was made on our website during the relevant time period, then it is possible that your information may not have been exposed in this incident.

What Information Was Involved?

We believe that the malicious actors had certain personal information about you such as name, address and/or date of birth and used that information to obtain your driver's license number via the quoting system tool. We regret this happened and sincerely apologize for any inconvenience and concern this causes you. We take our 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 will be provided by Cyberscout, a company specializing in fraud assistance and remediation 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.*

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.

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 it 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/

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