
State Farm Mutual Automobile Insurance Company, its affiliates and subsidiaries

February 18, 2022

Attorney General Brian E. Frosh
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

RE: Notice of Data Security Incident

Dear Attorney General Frosh,

As the Privacy Official of State Farm, I am writing to inform you of a data security incident that impacted five Maryland residents.

This incident involves vendor Rimkus Consulting Group, Inc. (RCG), a firm State Farm uses to fulfill engineering assignments for both auto and fire claims. On Friday, January 14, 2022, State Farm was notified by RCG that on or about July 2, 2021, they identified suspicious activity to three of their employees' email accounts. Upon discovery, RCG took steps to secure its network and engaged third-party digital forensic investigators to determine the nature and scope of the phishing attack.

The investigation revealed that the information accessed for the Maryland residents included their names, addresses, driver's license numbers, dates of birth, medical and health information.

State Farm provided notification in the form of a letter by US Mail to seven affected individuals as a result of this incident. Free credit monitoring was offered for a period of 12 months to all impacted individuals. A copy of the notification letter mailed on February 18, 2022 is attached.

If you have any additional questions, please contact me via email at luís.berrios.ux60@statefarm.com or by phone at 309-763-5189.

Sincerely,



Luis Berrios
Assistant Vice President/Privacy Official

State Farm Mutual Automobile Insurance Company, its affiliates and subsidiaries

One State Farm Plaza
Bloomington, IL 61710-0001

February 18, 2022

First Name Last Name
Street Address
City, State Zip Code

Dear First Name,

Notice of Data Breach

Your privacy is important to State Farm®, which is why we are writing about a data security incident that involves your personal information.

What Happened

This past July, Rimkus Consulting Group, Inc. ("RCG"), a company that provides engineering consulting services to assist State Farm with claims, noticed suspicious activity relating to certain RCG employees' email accounts. RCG quickly launched an investigation to determine the nature and scope of the activity and what information may have been affected. The investigation determined that an unknown actor accessed three RCG employee's email accounts, for limited periods of time, between June 25, 2021 and July 9, 2021.

RCG then worked with specialists to conduct a comprehensive review of information contained in the email accounts to determine what information was affected and to whom the information related. Upon completion of the third-party review, RCG then conducted a manual review of its records to confirm the identities of individuals affected by this event and their contact information to provide notifications. On or around December 30, 2021, RCG completed its initial review. Through the review, RCG determined that one of the email accounts contained information that was received from State Farm. RCG notified State Farm of the incident on January 14, 2022 and advised that your personal information may have been included within the contents of the email account at the time of compromise.

What Information Was Involved

RCG's investigation determined that at the time of the event, your (name, data elements) were stored within an impacted email account. To date, RCG has not received any reports of fraudulent misuse of information potentially impacted by this event.

What We Are Doing

The confidentiality, privacy, and security of your information are among our highest priorities. Upon learning of the activity, we immediately took steps to investigate the event.

What You Can Do

As a precaution, we are offering you a free one-year subscription to *myTrueIdentity*, a credit monitoring and identity theft protection service provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. This optional service will provide you with a copy of your credit report, monitor your credit files, notify you of certain suspicious activities that could indicate potential identity theft, and provide up to \$1,000,000 Identity Theft insurance for you and your covered family members if you are victims of identity theft.

- To learn more and enroll in an **online service**:
 - Go to www.mytrueidentity.com
 - In the "Enter Activation Code" space, enter the following 12-letter Activation Code
<<Insert 12-letter Activation Code>>
 - Follow the steps to receive your online credit monitoring service.

- To enroll for a **service delivered via mail**:
 - Call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422 (Available 24/7).
 - When prompted, enter the following 6-digit telephone pass code: **<<Insert 6-digit Telephone Pass Code>>**
 - Follow the steps to enroll in the offline credit monitoring service.

This offer will be available until **insert expiration date** (60 days from date on letter). For more information, please see the “Frequently Asked Questions” at the end of this letter.

- You should remain vigilant for the next 12 months by reviewing and monitoring your accounts and credit reports. If you do find suspicious activity on your accounts, call your local police or state Attorney General’s office to file a report. You have a right to obtain a police report if you are a victim of identity theft. Information about identity theft, fraud alerts, and security freezes can be obtained from the sources listed below.
- You are entitled to receive a free credit report from each of the three credit reporting agencies below every 12 months, and you may ask for a fraud alert on your credit report. A fraud alert tells creditors to contact you before any credit is issued or changes to your accounts are made, and generally stays in place for 90 days. For more information, contact one of the credit reporting agencies below:
 - **Equifax**: 800-525-6285; www.equifax.com; P.O. Box 105069, Atlanta, GA 30348-5069
 - **Experian**: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
 - **TransUnion**: 800-680-7289; www.transunion.com; P.O. Box 2000, Chester, PA 19016
- You may place a security freeze (also known as a credit freeze) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit report at the three national credit agencies without your consent. You must separately place a security freeze on your credit file at each credit agency listed above. Because the instructions differ from state to state, please contact the three credit agencies below to find out more information.
 - **Equifax**: 888-298-0045; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348-5788
 - **Experian**: 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
 - **TransUnion**: 888-909-8872; www.transunion.com; P.O. Box 2000, Chester, PA 19016
- Additional guidance on what identity theft is and how to report suspected fraudulent transactions can be obtained from the Federal Trade Commission (FTC):
 - **Phone**: 877-ID-THEFT (438-4338); or TTY: 866-653-4261
 - **Online**: www.ftc.gov/IDTheft and/or www.identitytheft.gov
 - **U.S. Mail**: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580
- Additional guidance on what identity theft is and steps you can take to avoid identity theft can be obtained from the Maryland Office of the Attorney General’s Consumer Protection Division.
 - **Phone**: 888-743-0023
 - **Online**: www.marylandattorneygeneral.gov
 - **U.S. Mail**: 200 ST. Paul Place, Baltimore, MD 21202

For More Information

I regret the inconvenience and concern this situation may have caused you. If you have questions about this incident, please contact your agent, or call us at 844-351-8206.

Sincerely,

Kelley Bott
Office of Privacy, Manager
State Farm®

Cc: State Farm Agent

Frequently Asked Questions

1 – Should I place a fraud alert with one of the credit reporting agencies?

The person affected should make that decision. You should consider that for a while, a fraud alert could slow down the credit application process. An initial fraud alert stays in place for 90 days.

2 – Should I obtain a free copy of my credit report?

There is no apparent downside to doing so. Obtaining a free copy of your credit report every 12 months is something all consumers should consider. To obtain your free credit reports from Equifax, Experian, and TransUnion. Go to www.annualcreditreport.com or call 1-877-322-8228.

3 – If I choose to take advantage of the *myTrueIdentity* credit monitoring service, how do I enroll?

- To enroll in an online service:
 - Go to www.mytrueidentity.com
 - In the “Enter Activation Code” space, enter the following 12-letter Activation Code provided for you in this letter.
 - Follow the steps to receive your online credit monitoring service.
- To enroll for a service delivered via mail:
 - Call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422 (Available 24/7).
 - When prompted, enter the following 6-digit telephone pass code provided for you in this letter.
 - Follow the steps to enroll.

4 – What if I have problems enrolling in the complimentary online *myTrueIdentity* credit monitoring service?

Contact TransUnion's *myTrueIdentity* toll-free customer service number at 844-787-4607. Their hours are: Monday-Thursday, 8:00 a.m.-midnight, and Friday-Sunday, 8:00 a.m.-8:00 p.m. (ET).

5 – What do I get with my TransUnion credit monitoring service enrollment?

- Unlimited access to your Credit Report, Credit Score and Credit Monitoring service for one year.
- Assistance if you become a victim of Identity Theft.
- Up to \$1,000,000 Identity Theft Insurance if you are a victim of Identity Theft (see www.mytrueidentity.com for details).