

To whom it may concern,

Pursuant to Bulletin 22-13, we are reporting the required details of a cybersecurity event.

Brief description of the nature of the security breach

In the ordinary course of business, we audit relevant employees' use of a third-party data service with which PGR does business. Through this audit, we discovered that an employee ran various searches for which we could ascertain no PGR business purpose. The search results revealed information about various people, including, without limitation, driver's license number and, in at least some cases, address, date of birth, 1st five digits of SSN, and vehicle information. We do not know what, if anything, the employee did with the information. But we found no indications that the employee saved any of the information in our system or attempted to send it outside of our network. We have received no complaints about identity theft or other fraud or misconduct committed using the information.

Number of Maryland residents being notified

Three

Sample copy of the notice being sent to consumers

Attached

What information has been compromised

Name and driver's license number, and possibly address, date of birth, first five digits of social security number, and vehicle information.

Any steps the business is taking to restore the integrity of the system

We terminated the person who ran these searches. That person no longer has any access to PGR systems or PGR's connection to the third-party data service.

Sincerely,

Heidi M. Smyksy
Progressive Insurance

Corporate Paralegal

W: 440.395.3767

E: Heidi_Smyksy@progressive.com



Date

Name

Address

City, State Zip

Dear [name]:

Progressive Casualty Insurance Company recognizes the importance of protecting personal information it maintains or to which it has access. We are writing to notify you of an incident that involved certain information about you. This letter explains the incident and measures we have taken. It also provides some additional steps you may consider taking in response.

What Happened?

A Progressive employee accessed information about you using Progressive's account with a third-party data provider. There was no Progressive business purpose for this activity. We do not know what, if anything, the employee did with the information. But we found no indications that she saved any of the information in our system or attempted to send it outside of our network. Though the person was employed by Progressive at the time of this activity, the person no longer works for Progressive or has access to its systems, data or account with the third-party data provider.

What Information Was Involved?

The information included your name and driver's license number, and might have included, without limitation, your address, date of birth, first five digits of your social security number, and vehicle information.

What We Are Doing.

Because of this, we are offering you free identity theft detection and restoration services. Detailed instructions for enrolling, along with information about these services, are enclosed.

What You Can Do.

Even if you do not subscribe to such services, you should remain vigilant for incidents of fraud and identity theft by reviewing financial account statements and monitoring free credit reports. You are entitled to receive a free copy of your credit report once each year from each of the three national credit reporting bureaus. Their contact information is enclosed.

You also may wish to consider placing a fraud alert or a security freeze on your credit report. A fraud alert instructs lenders to notify you if anyone tries to open a line of credit in your name. A security freeze prohibits the credit reporting bureaus from giving out information from your file without your permission. More information on both is enclosed.

If you ever believe that you may be a victim of identity theft, you should promptly file a report with law enforcement, including the police and the Federal Trade Commission (FTC). The FTC's contact information is enclosed.

Please refer to www.experian.com/fraudresolution for additional actions you can consider taking to reduce the chances of identity theft or fraud.

For More Information.

If you have any questions or need further assistance, please call our Credit Information Team at 1-800-876-5411. The team is available from 8 a.m. to 8 p.m. Eastern time Monday through Friday.

Thank you for your attention to this letter. Progressive takes privacy very seriously and regrets that this incident occurred.

Sincerely,

Edward P. Simms

Edward Simms
Assistant General Counsel
Progressive Casualty Insurance Company

Enclosure

FREE IDENTITY THEFT DETECTION AND RESTORATION SERVICES

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: 09/30/24 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your **activation code**:

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **09/30/24**. Be prepared to provide engagement number **B124841 B124843** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition.)

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

How to place a Fraud Alert or Security (Credit) Freeze on your credit report

Once a fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. The fraud alert will remain in effect for at least one year. During this time, if someone attempts to establish credit in your name, the creditor will be informed about the fraud alert and instructed to take extra steps to verify your identity. This may cause some delays if you are trying to obtain credit. For this reason, you may want to include a cell phone number where you can be easily reached.

With a security freeze on your credit file, potential creditors and other third parties cannot access your credit report unless you temporarily lift the freeze. If you want to freeze your credit, you must place the freeze with each credit reporting bureau. Credit reporting agencies cannot charge you to place, temporarily lift, or permanently remove a security freeze on your credit file.

To place a fraud alert or security freeze on your credit file, contact the three major credit reporting bureaus using the information provided below. More information about fraud alerts, security freezes, and avoiding identity theft is available from the FTC and the Maryland Office of the Attorney General (OAG) at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
1-877-FTC-HELP (1-877-382-4357)
www.ftc.gov

Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
(410) 576-6300
1-888-743-0023
www.marylandattorneygeneral.gov

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

If you see suspicious activity in your credit report, you should report it to the three major credit reporting bureaus:

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742
<http://www.experian.com/fraud/>

Equifax
Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348
1-888-378-4329
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

TransUnion
Fraud Victim Assistance
Department
P.O. Box 2000,
Chester, PA 19016-2000
1-800-680-7289
fvad@transunion.com
<https://www.transunion.com>