

Background

TransUnion is committed to the security and protection of consumer personal information. As a part of this commitment, TransUnion has teams that are continuously engaged in proactively monitoring, safeguarding and investigating questionable activity related to access to consumer information.

As a result of this ongoing monitoring and investigating, TransUnion teams flagged suspicious activity on various dates related to attempts to access certain credit files and consumer accounts for TransUnion products. Our team's initial assessment indicated that while the security of TransUnion's systems was not compromised, unauthorized actors may have used personal information **obtained from non-TransUnion sources** to impersonate consumers and attempt to access TransUnion products and services.

After identifying the suspicious activity, we conducted an in-depth investigation into these matters to determine if, and to what extent, personal information was viewed. We concluded our extensive examination into these matters on October 26, 2022, and although we have confirmed that the security of TransUnion's systems was not compromised, we do suspect that personal information, obtained from non-TransUnion sources, was used to access certain TransUnion products. The personal information involved varied, but included individual's names in addition to: Social Security number, date of birth, financial account number, driver's license number, and partially-redacted medical account number(s). Not all data elements were involved for all individuals.

Impacted Consumers

Our investigation determined that across all matters detailed below, a total of 10 Maryland residents were impacted. The breakdown of those figures, as well as the relevant dates, per matter are as follows:

<u>Matter #</u>	<u>Date Range of Suspicious Activity</u>	<u>Suspicious Activity Identified</u>	<u>Total Consumers Impacted</u>	<u>Maryland Residents Impacted</u>
1	5/13/21 to 6/22/22	July 19, 2022	4	1
2	3/22/22 to 6/26/22	July 12, 2022	214	1
3	1/16/22 to 7/15/22	August 3, 2022	213	8

What We Are Doing

TransUnion takes the protection of personal information seriously, which is why we engage in robust, proactive security measures such as cyber-intelligence investigations. As soon as we discovered the incident, we engaged in a dual-track effort to implement technical measures to block access to our services to potential unauthorized actors, and also to identify and notify individuals whose personal information we believe was accessed by unauthorized actors. We continue to enhance our security controls as appropriate to minimize the risk of any similar incident in the future.

On November 7, 2022, we notified impacted individuals, in the form of the letter attached, so that they can take additional measures to protect their personal information should they wish to do so. As a further precaution, we have arranged to offer complimentary identity theft protection and credit monitoring services to those impacted consumers. Please note that as TransUnion continues to refine our proactive security measures and cyber-intelligence investigations process, we anticipate a periodic practice of notifying consumers and state regulators of similar impersonation events going forward.

Contact Information

We would be happy to address any questions related to our notification related to these matters in further detail. Please direct any inquiries to:

Ryan Smith
Managing Counsel, Privacy
TransUnion LLC
555 West Adams St.
Chicago, IL 60661
Ryan.Smith@transunion.com

<Return Name>
<Return Address>
<City> <State> <Zip>



<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

To Enroll, please visit:
www.mytrueidentity.com
Activation code:

November 7, 2022

To <<First Name>> <<Last Name>>:

TransUnion LLC (“TransUnion”) is writing to make you aware of a risk to your personal data that we recently discovered. While this risk does not involve the compromise of any TransUnion systems, our proactive security measures did uncover that potential misuse of your personal information by unauthorized actors may have occurred. This letter provides information about our investigation and resources we are making available to you.

What happened?

TransUnion is committed to the security and protection of your personal information. As a part of this commitment, TransUnion has teams that are continuously engaged in proactively monitoring, safeguarding, and investigating questionable activity related to access to consumer information.

As a result of this ongoing monitoring and investigating, TransUnion teams flagged suspicious activity related to attempts to access certain credit files and consumer accounts for TransUnion products. Our team’s initial assessment indicated that while the security of TransUnion’s systems was not compromised, unauthorized actors may have used personal information obtained from non-TransUnion sources to impersonate consumers and attempt to access TransUnion products and services.

After identifying the suspicious activity on <<suspicious activity identified>>, we conducted an in-depth investigation into the matter to determine if, and to what extent, personal information was viewed. We concluded our extensive examination into the matter on October 26, 2022, and although we have confirmed that the security of TransUnion’s systems was not compromised, we do suspect that your personal information, obtained from non-TransUnion sources, was used to access using certain TransUnion products sometime between <<suspicious activity date range>>.

Those products contained personal information about you, which may include information from your credit file. TransUnion has taken steps to prevent further improper transactions and is working diligently to continually improve our protection capabilities to ensure your information is safeguarded, and criminal enterprises are disrupted. We are notifying you so that you can take additional measures to protect your personal information should you wish to do so. We have provided details of measures that we are undertaking, as well as steps that you can take to help protect your personal information below.

What information was involved?

The personal information involved included your name and your: <<impacted data element(s)>>.

What we are doing.

TransUnion takes the protection of personal information seriously, which is why we engage in robust, proactive security measures such as cyber-intelligence investigations. As soon as we discovered the incident, we engaged in a dual-track effort to implement technical measures to block access to our services to potential unauthorized actors, and also to identify and notify individuals whose personal information we believe was accessed by unauthorized actors. We continue to enhance our security controls as appropriate to minimize the risk of any similar incident in the future.

As a further precaution, we are offering you complimentary identity theft protection and credit monitoring services for a period of one year at no cost to you. Please see the attached Steps You Can Take to Help Protect Your Personal Information for enrollment details.

What you can do.

In addition to enrolling in complimentary credit monitoring services, the enclosed Steps You Can Take to Help Protect Your Personal Information includes additional information on general steps you can take to monitor and protect your personal information. We encourage you to remain vigilant against potential identity theft and fraud by carefully reviewing credit reports and account statements to ensure that all activity is valid. Any questionable charges should be promptly reported to the company with which the account is maintained.

For more information.

If you have any questions about this matter or would like additional information, please refer to the enclosed Steps You Can Take to Help Protect Your Personal Information or call toll-free (800) 916-8800. This call center is open Monday through Friday from 8:00 AM – 11:00 PM Eastern Time, except major holidays.

Sincerely,

TransUnion Consumer Relations

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Credit Monitoring Services

TransUnion is providing you with access to myTrueIdentity Online (TransUnion) Credit Monitoring services at no charge for one year from the date of enrollment.

Upon your completion of the enrollment process, you will have access to the following features:

- Unlimited online access to your TransUnion® credit report that can be refreshed daily
- Unlimited online access to your VantageScore® credit score from TransUnion, with analysis, that can be refreshed daily
- Daily TransUnion online credit monitoring and email alerts when critical credit information changes
- Up to \$1,000,000 identity theft insurance with no deductible (Policy limitations and exclusions may apply)
- Online access to TransUnion credit lock
- Online credit score trending
- Online credit dispute access
- Unlimited online access to credit management and identity theft prevention resources located in the online education center

How do I enroll for the free services?

To enroll in this service, go directly to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following 12-letter Activation Code <<enrollment code>> and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the myTrueIdentity online Credit Monitoring service anytime between now and November 30, 2022. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your myTrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

Review Your Account Statements

Carefully review account statements and credit reports to ensure that all of your account activity is valid. Report any questionable charges promptly to the financial institution or company with which the account is maintained.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission’s (“FTC”) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the “inquiries” section for names of creditors from whom you have not requested credit. Some companies bill under names other

than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the “personal information” section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. 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. Information that cannot be explained should also be reported to your local police or sheriff’s office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a free fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, GA 30348	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

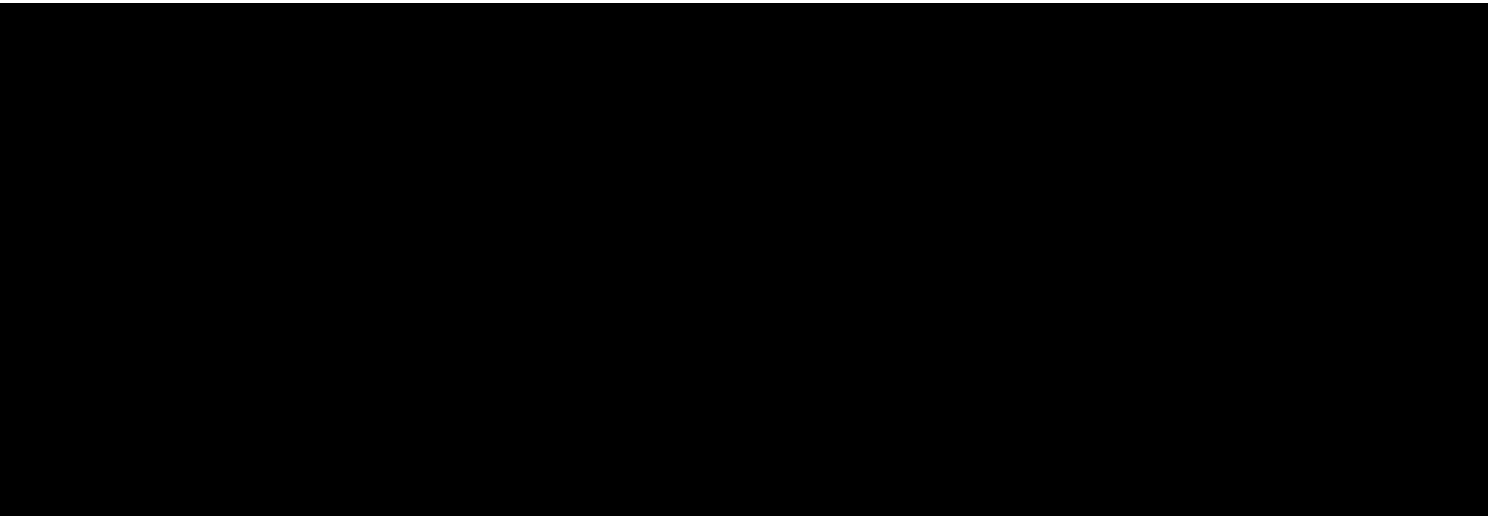
Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents of Maryland

You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, <http://www.marylandattorneygeneral.gov/>.

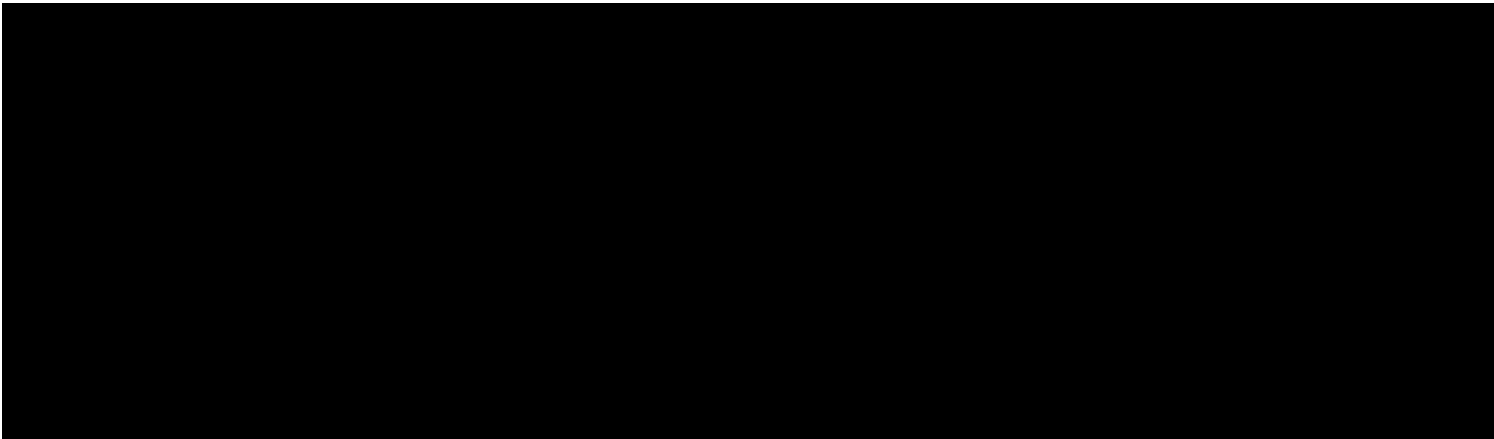


As a follow up to my earlier email, I'm reaching out on behalf of TransUnion to update a notice it provided on November 7, 2022. Since that time, TransUnion has identified an additional three impacted individuals from Maryland. As previously, those individuals will be notified and offered complimentary identity theft protection and credit monitoring services. To reiterate, these notifications are not the result of a compromise of TransUnion's systems, but instead involved unauthorized actors who appear to have used personal consumer information obtained from non-TransUnion sources to impersonate consumers and attempt to access their TransUnion consumer products.

As part of TransUnion's continued use of proactive security measures and cyber-intelligence investigations, we anticipate additional updates if more impacted individuals are identified. We would be happy to address any questions related to this update or the prior notice.

Thanks,
Bill

William Ridgway
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
155 N. Wacker Dr. | Chicago | IL | 60606
[T: 312.407.0449](tel:312.407.0449) | [C: 312.692.1606](tel:312.692.1606)



I'm writing on behalf of TransUnion to provide another update to the notice referenced below. Since the last update, TransUnion has identified an additional four impacted individuals from Maryland.

As previously, those individuals will be notified and offered complimentary identity theft protection and credit monitoring services. To reiterate, these notifications are not the result of a compromise of TransUnion's systems, but instead involved unauthorized actors who appear to have used personal consumer information obtained from non-TransUnion sources to impersonate consumers and attempt to access their TransUnion consumer products.

Please let me know if you have any questions.

Thanks,
Bill

William Ridgway
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
155 N. Wacker Dr. | Chicago | IL | 60606
[T: 312.407.0449](tel:312.407.0449) | [C: 312.692.1606](tel:312.692.1606)

From: Ridgway, William (CHI) <William.Ridgway@skadden.com>
Sent: Tuesday, December 20, 2022 3:21 PM
To: 'idtheft@oag.state.md.us' <idtheft@oag.state.md.us>
Subject: RE: Information Security Notice Update

As a follow up to my earlier email, I'm reaching out on behalf of TransUnion to update a notice it provided on November 7, 2022. Since that time, TransUnion has identified an additional three impacted individuals from Maryland. As previously, those individuals will be notified and offered complimentary identity theft protection and credit monitoring services. To reiterate, these notifications are not the result of a compromise of TransUnion's systems, but instead involved unauthorized actors who appear to have used personal consumer information obtained from non-TransUnion sources to impersonate consumers and attempt to access their TransUnion consumer products.

As part of TransUnion's continued use of proactive security measures and cyber-intelligence investigations, we anticipate additional updates if more impacted individuals are identified. We would be happy to address any questions related to this update or the prior notice.

Thanks,
Bill

William Ridgway
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
155 N. Wacker Dr. | Chicago | IL | 60606
[T: 312.407.0449](tel:312.407.0449) | [C: 312.692.1606](tel:312.692.1606)

From: Ridgway, William (CHI)
Sent: Tuesday, December 13, 2022 5:46 PM
To: 'idtheft@oag.state.md.us' <idtheft@oag.state.md.us>
Subject: Information Security Notice Update

I'm reaching out on behalf of TransUnion about a recent information security notice it submitted on Nov. 7 and would like to give a quick update on that. I'm happy to provide that via this account or be directed elsewhere as appropriate (or do so on a call).

Thanks,
Bill

William Ridgway
Partner
Skadden, Arps, Slate, Meagher & Flom LLP
155 N. Wacker Dr. | Chicago | IL | 60606
[T: 312.407.0449](tel:312.407.0449) | [C: 312.692.1606](tel:312.692.1606)

This email (and any attachments thereto) is intended only for use by the addressee(s) named herein and may contain legally privileged and/or confidential information. If you are not the intended recipient of this email, you are hereby notified that any dissemination,

distribution or copying of this email (and any attachments thereto) is strictly prohibited. If you receive this email in error please immediately notify me at (212) 735-3000 and permanently delete the original email (and any copy of any email) and any printout thereof.

Further information about the firm, a list of the Partners and their professional qualifications will be provided upon request.

=====