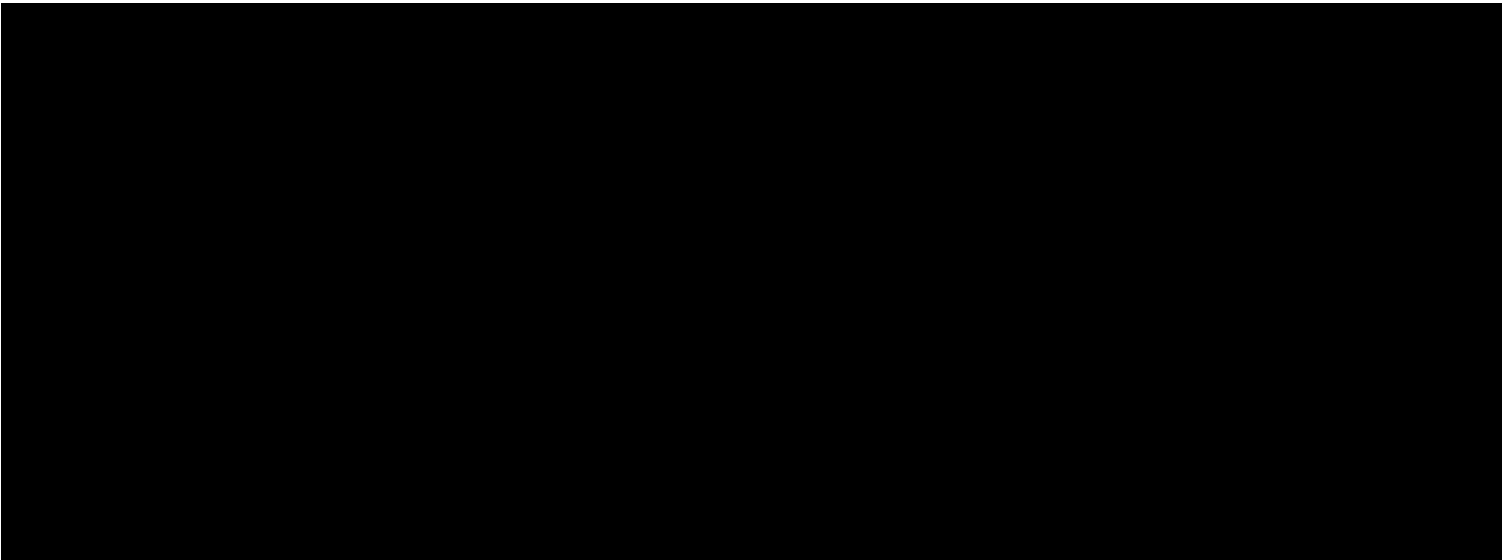




Good morning,

On February 6, 2024, TIAA Trust, N.A. became aware that online credentials were used by an unauthorized person to access two individuals' TIAA accounts. The unauthorized person accessed the accounts from January 1, 2024 to February 5, 2024 using the correct user IDs and passwords obtained through unknown means. From our investigation, the person obtained the credentials from a source other than our systems. This incident impacts two (2) Maryland residents who will both be receiving written notice of the event with an offer of free credit monitoring for 24 months. The individuals' account credentials were reset. We take this event and the security of the information in our care seriously.

Please see the attached sample notice to the individual.

Thank you,

Julia Olienyk, J.D.
Privacy Legal Analyst
Enterprise Privacy Office | Corporate & Technology Law
TIAA
8500 Andrew Carnegie Blvd
Charlotte, NC 28262
julia.olienyk@tiaa.org
www.tiaa.org
TIAA-CREF Individual & Institutional Services, LLC, Member FINRA and SIPC

REPORTING DATA EXPOSURE/PRIVACY INCIDENTS

Data exposure for all employees, customers, consumers, clients must be reported to the Fraud Servicing Team (except for Nuveen, TIAA Trust, and TIAA Bank).

For reporters from the NCC: use the '**Fraud Servicing**' option on the telephony toolbar transfer list.
For all non-NCC reporters: call **67-6017**.

The hours are weekdays 8 a.m. – 10 p.m. (ET) and for off hours, submit a digital report using the [TIAA Investigations Management System \(TIMS\)](#).
Reminder: Consultants on Genesys Cloud should be using the Favorites drop-down or Team Communicator. If the group you are looking for is not available, you must dial 980-867-6107.

Also see [Incident Reporting Job Aid](#)

This e-mail may contain confidential or privileged information.

If you are not the intended recipient, please notify the sender immediately and then delete it.

TIAA



Name
Title
Business Unit or Department
Tel: (XXX) XXX-XXXX ext. XX XXXX
Fax: (XXX) XX-XXXX
XXXXX@tiaa.org

Month XX, 202X

Name
Address
Address

Re: Notice of data **exposure**

Dear **Name**:

What happened

Protecting the privacy and security of your information is extremely important to us. For this reason, we previously contacted you by phone on XXXXXXXX XX, XXXX, to inform you that your online credentials were used by an unauthorized person to access your account. This letter summarizes our conversation, explains what we are doing in response, and how you can further protect your account.

The unauthorized person who accessed your account [on/between XXXXX and] XXXXXXXX used your correct user ID and password or other credentials to gain access. From our investigation, the person had your credentials from a source other than our systems.

What information was involved

While the unauthorized person had access to your online account, they had access to view your XXXX, XXXX, XXXX.

What we are doing

We take this event and the security of information in our care seriously. Upon learning about this event, we quickly shut down access to your account.

We also checked your accounts and either saw no indication of unauthorized activity or reversed it. We also initiated a password reset to ensure the unauthorized person no longer has access to your account. While we have not detected any indication of improper use of your information, we placed additional monitoring and protection on your account. Consequently, you may be asked to provide additional information during the authentication process to your TIAA account in the future.

As an added precaution, to help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for **two (2) years**. For more information about how to take advantage of this offer, see the information under "How you can sign up for credit monitoring" below.

What you can do

As a measure of good security practices, we recommend that you always check your computer for viruses and remove them.

Then, please create a new user ID and password to access your TIAA accounts online and any other account for which you use the same credentials. Your new credentials should be a random combination of letters and

numbers and should be only used for your TIAA online account. For added protection we recommend you take the following actions:

- Download the TIAA mobile app on your cellular phone and use it to conduct financial transactions. Please note, TIAA will never call you to request your personal information or one-time passcode; if you receive such a call, please treat it as a fraud attempt.
- Enable the use of a one-time passcode each time you access your TIAA online account.
- Place a personalized password to access your TIAA account via our phone center, for an added level of verbal security.*

We also strongly encourage you to review your online credentials in non-TIAA websites and change them if you were using the same old TIAA user ID and password combination. This will minimize the risk of the unauthorized person's use of your old credentials in non-TIAA accounts. Your user IDs and passwords in each of your online accounts outside TIAA should be unique to each site and consist of random combinations.

We recommend taking advantage of the offer of credit monitoring detailed below. Even if you do not take advantage of the offer, we advise that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

For more information

Please feel free to contact me directly at (800) XXX-XXXX, extension XX XXXX if you have any questions concerning this matter.

Protecting the privacy and security of your information is extremely important to us. For more information, you can visit the Privacy and Security links on TIAA.org.

Please know that we value your trust and take this matter very seriously.

Sincerely,

XXXXXXX
XXXXXXXXXX

* Please note that this password is different from the one that you use to login to your account on TIAA.org

How you can sign up for credit monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for **two (2) years** 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [membership duration] membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by [Enrollment End Date]** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/RR3Bplus>
- Provide your **activation code: [activation code]**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [Experian TFN] by [enrollment end date]. Be prepared to provide engagement number [engagement number] as proof of eligibility for the Identity Restoration services by Experian.

Additional Details Regarding Your Two-Year 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.

** 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.

- **Lost Wallet:** Provides assistance with canceling/replacing lost or stolen credit, debit, and medical cards.
- **Child Monitoring:** For 10 children up to 18 years old, Internet Surveillance and monitoring to determine whether enrolled minors in your household have an Experian credit report are available. Also included are Identity Restoration and up to \$1M Identity Theft Insurance.**

Other Important Information Including Information about Identity Theft Prevention

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your free credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-916-8800
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand or identify information that you believe is not correct, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax® Information Services
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
www.equifax.com/personal/credit-report-services

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion® (FVAD)
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.);
- 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; and

- 8) Other personal information as required by the applicable credit reporting agency;

Note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well. If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax® Information Services

P.O. Box 105069
Atlanta, GA 30348-5069
1-800-525-6285

[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742

[www.experian.com/
fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

[www.transunion.com/fraud-
alerts](http://www.transunion.com/fraud-alerts)

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. This notification was not delayed due to law enforcement investigation.

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

For residents of Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Virginia, and Vermont: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also

order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement, or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed above.

For residents of the District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Maryland, New York, North Carolina, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Office of the Attorney General for the District of Columbia:
400 6th Street NW | Washington, D.C. 20001 | 1-202-727-3400 | oag@dc.gov

Maryland Office of the Attorney General:
Consumer Protection Division | 200 St. Paul Place | Baltimore, MD 21202 | 1-888-743-0023
Marylandattorneygeneral.gov

New York Office of the Attorney General:
Consumer Frauds & Protection Bureau | 120 Broadway - 3rd Floor | New York, NY 10271
breach.security@ag.ny.gov

North Carolina Office of the Attorney General:
Consumer Protection Division | 9001 Mail Service Center | Raleigh, NC 27699 | 1-877-566-7226
www.ncdoj.com

Rhode Island Office of the Attorney General:
Consumer Protection | 150 South Main Street | Providence RI 02903 | 1-401-274-4400
www.riag.ri.gov

For residents of Rhode Island: You have the right to obtain a police report if you are a victim of identity theft. There [are/is] approximately [#] Rhode Island resident[s] that may be impacted by this event.