



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:

We are writing to notify you of an incident that involves some of your personal information. We want to assure you that we take this matter very seriously, as protecting the privacy and security of your information is extremely important to us.

As described in more detail below, we would like to let you know what happened, how we have responded to protect your information against a risk of identity theft or fraud and important steps you can take to further protect it.

Specifically, we are offering you two years of complimentary credit monitoring/identity theft protection and encourage you to sign up for it as soon as practicable, as explained in the section entitled "Activate your monitoring services" below.

We previously spoke to you on XXXXX XX, XXXX about this incident. We encourage you to remain vigilant by reviewing your financial account transactions and statements for unauthorized transactions and immediately notifying your relevant financial provider if you detect any. We also recommend that you implement the steps listed in the section entitled "Monitor your accounts below" and obtain free credit reports from consumer reporting agencies.

What happened

An unauthorized individual accessed your account[s] [on/between XXXXX and XXXXXXXX]. This unauthorized person used information obtained from a source other than TIAA to initiate a reset of your online access account credentials.

What information was involved

Our investigation of the incident reveals that the unauthorized person viewed your XXXX, XXXX, XXXX while in your account.

What we are doing

As soon as we became aware of an issue relating to your account, we promptly investigated it, confirmed that your personal information was involved, and reached out to you. We also checked your accounts and either saw no indication of unauthorized activity or reversed it.

Additionally, we initiated a password reset to ensure the unauthorized person no longer has access to your account. We have also placed additional authentication monitoring to your TIAA account[s].

We are offering you complimentary access to Experian IdentityWorksSM for **24 months**. Among other features, this service monitors the use of your personal information in new financial accounts and alerts you to determine whether they were opened without your authorization. Please sign up for this offer using the instructions in the section below entitled “Activate your monitoring services.”

What you can do

In addition to signing up for our complimentary offer of credit monitoring, we strongly urge you to do the following:

- ☐ Review each of your online accounts and create strong and unique passwords for each.
 - “Strong” passwords consist of a random combination of letters and numbers and, where permitted, symbols.
 - Unique passwords for each online account prevent unauthorized persons to access your other online accounts after compromising just one.
- ☐ Implement a unique password at TIAA’s National Contact Center to access your TIAA account by phone (again, avoid re-using your online login password).
- ☐ Download the TIAA mobile app on your mobile device to conduct your TIAA financial transactions.
- ☐ Enable the use of a one-time passcode on each of your online accounts.
- ☐ Stay alert for online scams by assessing suspicious emails or websites,
- ☐ Regularly check your online accounts for unauthorized transactions and dispute them immediately.
- ☐ Close any online accounts that you no longer use.
- ☐ Contact the credit reporting bureaus (Experian, Equifax, TransUnion) if you know of or suspect any unauthorized accounts or fraudulent transactions and:
 - Dispute them immediately;
 - Request that the credit reporting agency remove the fraudulent transaction from your credit report; and
 - Contact your state Attorney General, police, or the Federal Trade Commission (FTC) .
- ☐ Place a credit freeze or credit fraud alert to prevent unauthorized accounts being opened in your name.

Contact details are provided in the **Monitor your accounts** and **Additional information** sections below.
For more information

For more useful tips, please visit the Privacy and Security links on TIAA.org.

Please know that we value your trust and take this matter very seriously. If you have any questions, please feel free to contact me directly at (8XX) XXX-XXXX, extension XX XXXX

Sincerely,

XXXXXX
XXXXXXXXXX

Steps you can take to help protect personal information

Activate your monitoring services

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 **24 months** 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 **24-month** 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 24-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.
- **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.**

* 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.

Monitor your accounts

Under U.S law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report. If you find information related to fraudulent transactions on your credit report, you can submit a request to the credit reporting bureaus to remove those transactions.

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

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

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. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338) and TTY 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft and fraud. Please note that to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general.

For residents of the District of Columbia, Iowa, Kentucky, Maryland, New York, North Carolina, and Oregon:

You may contact your Attorney General for additional information about avoiding identity theft. You may use the following information to contact your attorney general:

Office of the Attorney General Office of Consumer Protection 400 6th Street, NW Washington, DC 20001 (202) 442-9828 www.oag.dc.gov	Office of the Iowa Attorney General Hoover State Office Building 1305 E. Walnut Street Des Moines, IA 50319 (515) 281-5926 / (888) 777-4590 www.iowaattorneygeneral.gov	Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 (410) 528-8662 www.marylandattorneygeneral.gov	Kentucky Attorney General Office of Consumer Protection 1024 Capital Center Drive Suite 200 Frankfort, KY 40601 1-502-696-5389 www.ag.ky.gov
New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway, 3rd Floor New York, NY 10271 (800) 771-7755 www.ag.ny.gov	New York Department of State Division of Consumer Protection 99 Washington Avenue Suite 650 Albany, New York 12231 (800) 697-1220 www.dos.ny.gov	North Carolina Department of Justice 9001 Mail Service Center Raleigh, NC 27699-9001 (919) 716-6000 www.ncdoj.gov	Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 (877) 877-9392 www.doj.state.or.us

For residents of Hawaii, Iowa, Maryland, Michigan, Missouri, New Mexico, North Carolina, Virginia, Vermont, and Wyoming:

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 Massachusetts: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf

For residents of Rhode Island: You have the right to obtain a police report if you are a victim of identity theft. You may file a police report by contacting local or state law enforcement. Fees may be required to be paid to consumer reporting agencies when requesting a security freeze. There [are/is] approximately [#] Rhode Island resident[s] that may be impacted by this event. Rhode Island Office of the Attorney General Consumer Protection Division, 150 South Main Street Providence, RI 02903, (401) 274-4400, www.riag.ri.gov