TIAA Bank

29088

[Return Address Line 1]
[Return Address Line 2]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

[Date]

RE: Notice of TIAA Bank Data Security Incident

Dear [First Name] [Last Name]:

We are writing to notify you of an incident at TIAA, FSB ("TIAA Bank") that may have involved your personal information and to inform you of what we are doing in response, how you can further protect your accounts, and how you can enroll in the credit monitoring and identity protection tools that we are making available to you.

What Happened? On December 13, 2022, our internal security tools alerted us to suspicious activity potentially implicating a former employee who had access to personal information as part of their job responsibilities. We immediately began a thorough investigation and implemented our incident response protocols, leading us to engage law enforcement.

Our records show that you had an interaction with this person last year, but we want to assure you that we have not seen any indication of fraudulent activity on your bank account or misuse of your personal information at TIAA Bank. At this time, we would like to make you aware of the incident and provide you tools and information to help protect your identity, given that we cannot rule out the possibility that your personal information has been compromised.

In addition to engaging law enforcement, we are implementing controls to help prevent this type of activity in the future. We will continue to monitor your account for suspicious activity; please take the steps outlined in this letter to protect your accounts and contact us immediately if you suspect any fraudulent activity.

What Information Was Involved? The employee had access to your personal information as part of their employment with TIAA Bank. This information includes some or all of the following: your name, address, telephone number, financial account information, debit card information (including your card security code), TIAA Bank security code, mother's maiden name, email, UserID, date of birth, and your Social Security Number. The employee would not have had access to your online login password as part of their employment.

What We are Doing.
We take the security of personal information very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by performing immediate remediation activities, and we are implementing additional controls, training, and coaching.

In addition, to help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months, as set forth below.

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 Experian Identity Restoration is available to you for 24 months from the date of your enrollment 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 [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 Experian 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 October 1, 2023. Be prepared to provide engagement number **[CODE]** as proof of eligibility for the Experian Identity Restoration services.

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 file 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**.

What You Can Do. Please review the enclosed *Information about Identity Theft Protection* for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered. We also recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. Contact us right away at 1-888-882-3837 if you suspect any unauthorized activity involving your financial accounts or if you experience any suspicious activity from an individual purporting to be from TIAA Bank.

For added protection we recommend you take the following actions, if you have not already done so:

- Log in to your account and set your communication preferences to enable real-time email and text alerts for your financial accounts. Alerts can help you monitor your account balance and transactions and inform you of recent changes so you can take action immediately to help avoid fraud or unexpected charges.
- Enable multi-factor authentication, which requires that you enter a one-time passcode each time you access your TIAA Bank online account.
- Keep your contact information current (including your cell phone number and email address).
- If you receive a suspicious call, text or email from someone claiming to be from TIAA Bank, do not respond, click links or open attachments. If this has happened to you, contact us right away at 1-888-882-3837.
- Do not provide your personal secure information to an unsolicited caller. We will never initiate a call asking you to provide your full account number, online/mobile banking passwords, PINs or complete Social Security number over the phone, except limited instances when we are returning a call at your request.

- Never respond to a phone call or voice mail service asking you to verify account information or reactivate a bank service, even if the caller recites some of your account information to you. They may have obtained the information from another source and are enticing you to provide additional details that would help them access your accounts.
- Check your computer for viruses and remove them.
- Create a new user ID and password to access your TIAA Bank accounts online. Your new credentials should be a random combination of letters and numbers and should be only used for your TIAA Bank online account. We strongly encourage you to review your online credentials in non-TIAA Bank websites, including your email services, and change them if you were using the same old TIAA Bank user ID and password combination. This will minimize the risk of the unauthorized person's use of your old credentials in non-TIAA Bank accounts. Your user IDs and passwords in each of your online accounts outside TIAA Bank should be unique to each site.

For additional steps you can take to protect your accounts and for more information about our security practices and the tools available to you, please visit tiaabank.com/security.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call [Experian TFN] toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number, [CODE]. Please also visit the Privacy and Security links on tiaabank.com. Please know that we value your trust and take this matter very seriously.

Sincerely,

[Your Signature Graphic]

[Organization Contact, Title]
[Organization Name]

* 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.

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your 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®	**Experian**	**TransUnion®**
P.O. Box 740241	P.O. Box 9701	P.O. Box 1000
Atlanta, GA 30374-0241	Allen, TX 75013-9701	Chester, PA 19016-1000
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	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, 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	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com/personal/ credit-report-services	www.experian.com/ freeze/center.html	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) Other personal information as required by the applicable credit reporting agency;

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	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com/personal/credit-report-services	www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert

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 Federal Trade Commission.

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. For more information about the Fair Credit Reporting Act, visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed above.

For residents of Maryland, New York, North Carolina, District of Columbia, 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.

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

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 27699-9001
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

D.C. Attorney General
441 4th Street NW
Washington, D.C. 20001
1-202-727-3400
www.oag.dc.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of Rhode Island: There were six Rhode Island residents notified in this incident.