



VIA EMAIL

Maryland Insurance Administration support@marylandinsurance.zendesk.com
Idtheft@oag.state.md.us

June 7, 2024

Re: Notice of Data Security Incident

To Whom It Concerns:

We are writing to provide you with an update to a previously reported cybersecurity incident regarding a service disruption that Infosys McCamish Systems, LLC ("IMS"), a key administrative vendor of Teachers Insurance and Annuity Association of America and TIAA-CREF Life Insurance Company (collectively "TIAA"), experienced last November.

Nature of Data Security Incident

TIAA uses IMS for administrative support services relating to TIAA's life insurance and after-tax annuity businesses. On or around November 2, 2023, IMS was impacted by a cybersecurity incident which resulted in a disruption of their operational support to TIAA. An unauthorized party gained access to IMS systems and data. IMS promptly took steps to isolate and disconnect impacted systems. TIAA similarly terminated connections between our systems and IMS to protect our systems from potential harm. TIAA cybersecurity teams scanned our systems and did not identify any data or system compromise.

IMS retained a third-party firm to investigate and assist with IMS's recovery plan and ultimately implemented additional security controls and restored full services, allowing TIAA to return to processing transactions in December 2023. IMS has since found no evidence of continued threat actor access in its environment.

IMS also retained a third-party e-discovery firm to investigate what data was impacted and to whom it may belong.

Notice to Maryland Residents

Beginning on March 7, 2024, while IMS' e-discovery investigation was ongoing, TIAA began proactive notification to **13,485 Maryland** residents informing them that some of their data might be impacted, offering two (2) years free credit monitoring, and advising them how to protect their data. The notification also provided the details of the incident, additional information on steps individuals can take to protect against identity theft and fraud, and contact information individuals may use should they have any questions or concerns. We also provided a toll-free number for individuals to contact

with questions or concerns regarding this incident and the services being offered. A sample copy of the customer notification letter is included with this letter.

Latest Status

On May 28, 2024, IMS notified us that their e-discovery investigation concluded and confirmed that personal information that IMS processed on TIAA's behalf was subject to unauthorized access and acquisition. On May 29, IMS provided to TIAA a data file including the names of around 16,713 individuals; however, on May 31, IMS informed TIAA that the data file is: 1) underinclusive, potentially omitting names of impacted individuals who are TIAA customers but whom IMS was unable to match with TIAA; and 2) overinclusive, potentially including the names of impacted individuals with no relationship to TIAA. TIAA requested that IMS clean and enhance the data file and immediately return it to TIAA, as the data file originally provided by IMS did not include sufficient information that would enable TIAA to identify whether the named individual had a relationship with TIAA.

Since receiving confirmation from IMS on May 28th that its e-discovery investigation was complete and that TIAA personal information was impacted, we are working diligently to validate the data file and provide required notifications to **Maryland** residents. Neither TIAA nor IMS is aware of any misuse of specific personal information.

Regrettably, there is a possibility that, even with the clean and enhanced data file from IMS, we may not be able to confirm with substantial certainty the full extent of TIAA's impacted population or the accurate number of impacted **Maryland** residents. As we previously reported, TIAA already made proactive outreach to individuals whose data IMS processed on behalf of TIAA that could have been impacted by this incident, providing them with notice of what happened and offering complimentary identity protection services. To the extent McCamish is unable to match an impacted individual to TIAA or another institution, it has committed to provide appropriate regulatory and individual notifications required by law.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security incident, please contact us at (704) 988-6252 or lsey@tiaa.org.

Sincerely,



Louis Senay
Managing Director, Head of Supervisory Affairs
Teachers Insurance and Annuity Association of America



TIAA
730 Third Avenue
New York, NY 10017

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: Security Incident – Credit Monitoring

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to update you on the cybersecurity incident experienced by TIAA and TIAA Life's administrative support services vendor, Infosys McCamish Systems, LLC ("IMS"), which resulted in an operational outage during the month of November. We previously informed you about this outage in November 2023 and the subsequent restoration of services in December 2023. As of the date of this letter IMS has provided us with information indicating that personal information for some of our customers was impacted, but IMS has not yet confirmed whether your specific personal information has been impacted. However, out of an abundance of caution, we are providing you with more information about what happened, what data may have been impacted, and tools to help you protect against possible identity theft or fraud.

What Happened: On or around November 2, 2023, IMS was impacted by a cybersecurity incident in which an unauthorized party gained access to IMS systems and data. IMS immediately disabled the systems and retained a third-party forensics firm to investigate and assist with IMS's recovery plan. IMS implemented additional security controls and restored full services in December and has found no evidence of continued threat actor access in its environment.

IMS also retained a second third-party e-discovery firm to investigate what data was impacted, and to whom it may belong.

What Information Was Involved While we have received confirmation that personal information for some of our customers was impacted, the third-party firm engaged by IMS is currently conducting a review to determine whether your specific personal information was impacted. This review is ongoing. We will notify you in the event IMS determines that your specific personal information was impacted. The types of data that could be impacted varies by individual and could include some or all the following: name, Social Security number, date of birth, life insurance policy number, annuity contract number, financial account number, and medical information that you may have provided to TIAA or TIAA Life in relation to a life insurance policy.

What We Are Doing: Neither TIAA nor IMS is aware of any actual access to or misuse of your specific personal information. However, in an abundance of caution, IMS has secured Kroll's services to provide identity monitoring services **at no cost to you** for 2 years from the date of your activation. Kroll is a risk mitigation and response firm that helps individuals monitor for indicators of potential fraud or identity theft. Your identity monitoring services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. These services will expire at the conclusion of the complimentary 2-year period and will not automatically renew.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your identity monitoring services, you can visit info.krollmonitoring.com.

Please have your Membership Number located in this letter ready when calling.

Additional information describing your services is included with this letter.

What You Can Do: We recommend you take the following steps to help protect your personal information:

- Promptly review your credit reports and account statements over the next 24 months and notify your financial institution of any unauthorized transactions or incidents of suspected identity theft.
- Activate the complimentary identity monitoring service offered above.

We also recommend that you review the additional information about ways to help protect your identity or any additional rights you have depending on where you live, both provided in **Attachment A** on the following pages.

For More Information. Should you have any questions regarding this incident, please contact IMS' dedicated call center number by dialing (866) 992-9742, Monday – Friday between 8 am – 5:00 pm CT, excluding major U.S. holidays.

We apologize for any concern or inconvenience this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Ali Iqbal".

Ali Iqbal
President
TIAA-CREF Life Insurance Company

ENC: Attachment A: Additional Information on Protecting Your Information and State Law Information

Attachment A: Additional Information on Protecting Your Information and State Law Information

Monitor Your Accounts

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
1-800-888-4213
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 creditors 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 identified above.

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: 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; and other personal information as required by the applicable credit reporting agency. If you request a credit freeze online or by phone, the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file. If you request a lift of the credit freeze online or by phone, 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, the credit reporting 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 credit file at no cost. An initial fraud alert lasts 1-year. 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 lasts 7 years. Should you wish to place a fraud alert, please contact any one of the major consumer reporting agencies listed above. The agency you contact will then contact the other two credit agencies.

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

For residents of the District of Columbia, Iowa, Maryland, New York, North Carolina, Oregon and Rhode Island

You may contact your Attorney General for additional information about avoiding identity theft. If you are a Rhode Island resident, you may also file a police report by contacting local or state law enforcement agencies. 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	Oregon Department of Justice 1162 Court Street NE Salem, OR 97301-4096 (877) 877-9392 www.doj.state.or.us
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	Rhode Island Office of the Attorney General Consumer Protection Division 150 South Main Street Providence, RI 02903 (401) 274-4400 www.riag.ri.gov

For residents of Kentucky: The Kentucky Attorney General – Office of Consumer Protection may be contacted at: 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601; 1-800-804-7556; and <https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Identity-Theft.aspx>.

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 or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

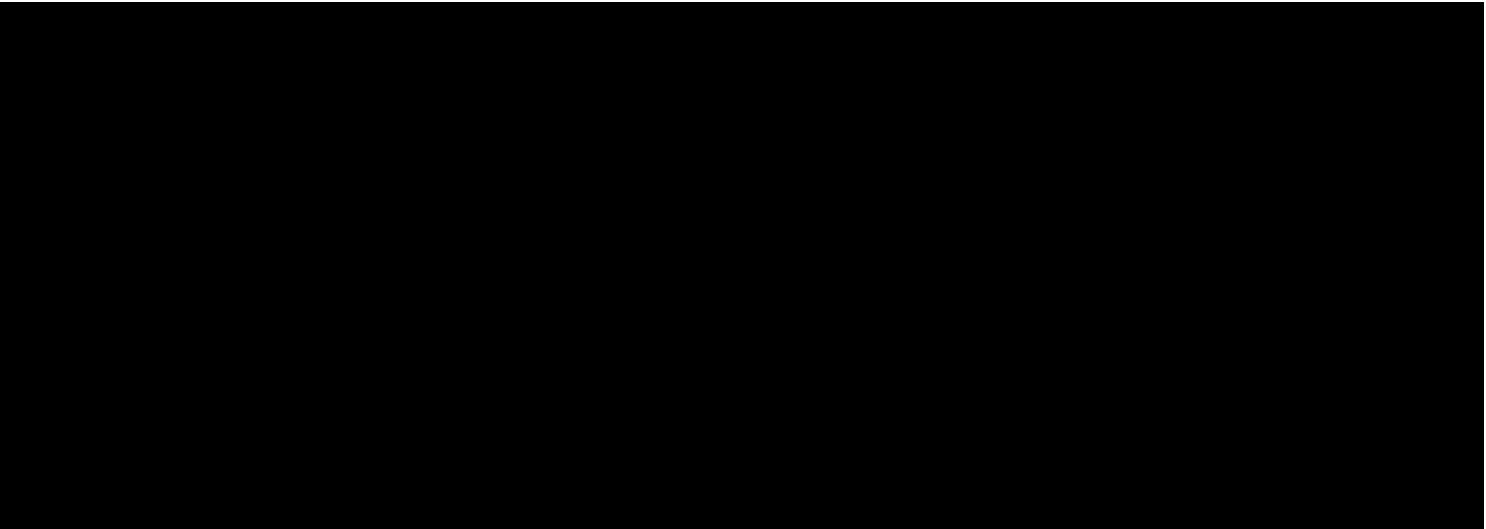
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.



Good afternoon,

Following is another update regarding the previously reported cybersecurity incident at Infosys McCamish Systems, LLC (IMS), that took place on November 2, 2023.

As previously reported, beginning on March 7, 2024, while IMS' e-discovery investigation was ongoing, TIAA began proactive notification to potentially impacted Maryland residents informing them that some of their data might be impacted, offering two (2) years free credit monitoring, and advising them how to protect their data.

On May 28, IMS notified us that their e-discovery investigation concluded and confirmed that personal information that IMS processed on TIAA's behalf was subject to unauthorized access and acquisition. On May 29, IMS provided to TIAA a data file including the names of approximately 16,700 individuals, of which only about 461 are Maryland residents; however, on May 31, IMS informed TIAA that the data file is: 1) under-inclusive, potentially omitting names of impacted individuals who may be TIAA customers but whom IMS was unable to conclusively match with TIAA; and 2) over-inclusive, potentially including the names of impacted individuals with no relationship to TIAA.

The data file provided by IMS on May 29 did not include sufficient information to enable TIAA to identify whether the named individual had a relationship with TIAA. TIAA requested that IMS clean and enhance the data file and immediately return the revised file to TIAA. Since May 29, we have been working diligently to validate the information within the data file. It is possible that, even with the clean and enhanced data file from IMS, we may not be able to confirm with substantial certainty the full extent of TIAA's impacted population or the accurate number of impacted residents.

On July 10, following an in-depth analysis of the data provided by IMS, TIAA's legal counsel reached the conclusion that a legal "breach" standard has been met for approximately 457 Maryland residents, to whom we will provide additional notifications. As we continue our data analysis and perform de-duplication, it is possible this number will decrease.

Additionally, IMS is issuing breach notification letters for affected individuals where they are unable to determine the specific IMS client from which the data originated; TIAA is not mentioned in these notifications. However, some TIAA retail and TIAA Life customers may receive IMS breach notifications directly. The identity theft protection services provided by IMS through Kroll include two years of complimentary credit monitoring and call center services to assist in registration.

Neither TIAA nor IMS is aware of any misuse of specific personal information.

Let us know if you have any questions or need any additional information.

Sincerely,
Louis Senay
Managing Director, Supervisory Affairs

From: Senay, Lou

Sent: Friday, June 7, 2024 3:28 PM

To: Maryland Insurance Administration <support@marylandinsurance.zendesk.com>; ldtheft@oag.state.md.us

Subject: RE: TIAA / TC Life - McCamish Cybersecurity Event - Update

Good afternoon,

As promised, following is another update as we continue to learn more about the nature of the data that was compromised. Please see attached notification letter we are sending to appropriate state regulatory authorities. I'd like to point you to the section titled **Latest Status**. Within you will see we unfortunately still do not have a clear understanding of the number of TIAA customers confirmed to be impacted, nor is it likely we ever will.

We continue to work with IMS to analyze whatever data is available and will keep you updated if there are any material changes.

Sincerely,
Louis Senay
Managing Director, Supervisory Affairs

From: Senay, Lou

Sent: Thursday, May 30, 2024 3:30 PM

To: Maryland Insurance Administration <support+id194@marylandinsurance.zendesk.com>

Subject: RE: TIAA / TC Life - McCamish Cybersecurity Event - Update

We are writing to provide an update to a previously reported cyber event regarding a service disruption that occurred at a key administrative vendor of Teachers Insurance and Annuity Association of America and TIAA-CREF Life Insurance Company (collectively "TIAA").

Late on May 28, the vendor, Infosys McCamish Systems, LLC ("IMS") notified us that their e-Discovery investigation has concluded and confirmed that personal information processed by IMS on TIAA's behalf was subject to unauthorized access and acquisition. We have requested the list of impacted individuals associated with our organization and the impacted data elements. At this time, we are unable to determine the actual number of impacted residents in Maryland.

We will provide additional updates and any notifications required by law as additional information becomes available. Until such time, please don't hesitate to let us know if any questions.

Sincerely,
Louis Senay
Managing Director, Supervisory Affairs
(704) 562-7742

From: Senay, Lou

Sent: Wednesday, February 14, 2024 9:40 AM

To: Maryland Insurance Administration <support+id194@marylandinsurance.zendesk.com>

Subject: TIAA / TC Life - McCamish Cybersecurity Event - Update

Dear Commissioner Birrane, Hope all is well. Following is an update related to the McCamish Cybersecurity event.

Since our last correspondence on November 13, 2023.

- McCamish established a clean operating environment for its return to operations.
- Our operations resumed on December 8, 2023, and we are caught up on processing the backlog of transactions.
- Recently, McCamish identified certain TIAA / TC Life files that were impacted. Based on the names of those files, it is possible that personal information for some of our customers was exfiltrated.

- McCamish has engaged an eDiscovery team to review and investigate the data in potentially stolen files and to determine, to the extent possible, the scope of impacted personal information of TIAA/TC Life customers. We are told we won't know the results of this investigation until the July timeframe.
- It is unlikely we will ever be able to determine with certainty the exact scope of personal information that may have been compromised. While the information impacted varies from individual to individual, it could include some or all of the following: name, social security number, date of birth, life insurance policy number, annuity contract number, financial account number, and medical information that may have been provided to TIAA or TC Life in relation to a life insurance policy.
- At this time, we are unable to confirm specifically what data was accessed or acquired without authorization. However, out of an abundance of caution, we have decided to send voluntary notices on TIAA / TC Life letterhead to potentially impacted TIAA / TC Life customers and offer them free identity theft protection services for two years, offered by McCamish. We are working through the final edits for these notices, and we will be mailing the letters to customers once completed.
- We continue to work with McCamish and our internal teams to ensure we are reaching out to the appropriate customers. As of today, the estimated number of potentially impacted TIAA / TC Life customers that are residents in your state who will receive a courtesy notification is 13,485. We anticipate mailing these letters by the end of February.

As we learn more we will continue to keep you updated should anything materially change.

I hope this update is helpful. Please let us know if you have any questions or need any additional information.

Sincerely,
 Louis Senay
 Managing Director, Supervisory Affairs
 (704) 988-6252

From: Maryland Insurance Administration <support@marylandinsurance.zendesk.com>
Sent: Monday, November 13, 2023 7:03 PM
To: Senay, Lou <LSenay@tiaa.org>
Subject: [Request received]

CAUTION: This email originated from outside of the TIAA network. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Your request (194) has been received and is being reviewed by our staff.

To add additional comments, reply to this email.

Thank you,

Maryland Insurance Administration

This email is a service from Maryland Insurance Administration. Delivered by [Zendesk](#)

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
