TRAVIS COUNTY
CREDIT UNION

P.O. Box 301744
Austin, TX 78703

July 29, 2026

VIA U.S. MAIL

[NAME]
[ADDRESS]
[CITY, STATE, ZIP]

Dear [NAME],

We are writing to provide you with information regarding a data security incident (the “Incident”) experienced by Travis County Credit Union (the “Credit Union” or “we”) that may have involved your personal information (“Information”). This letter provides you with information about this Incident, our response, and where to direct your questions. To allow for additional safety measures, we have also provided steps you can take to protect your Information, which include an offer for 24 months of credit monitoring at no cost to you.

**What Happened?**

On March 3, 2026, we became aware of suspicious activity within our email environment after identifying a limited number of unauthorized emails. Upon discovering this, we promptly initiated an investigation and took steps to identify, contain, and remediate any unauthorized activity. These measures included changing passwords, revoking session tokens, and resetting multifactor authentication. We also engaged experienced data security and privacy professionals to assist in conducting a thorough forensic investigation.

The forensic investigation determined that an unauthorized actor accessed a limited number of Credit Union email accounts. Due to the swift response of our team, the Incident was contained promptly, and no further unauthorized activity was identified. Through our investigation, we identified that emails containing your Information were potentially accessed and/or acquired by an unauthorized actor. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

**What Information Was Involved?**

We may have collected your Information because you received financial services from the Credit Union. Based on our findings from the investigation, the following types of Information may have been impacted: name, <<Data Elements>>. There is currently no evidence that any Information has been misused for identity theft or fraud in connection with the Incident.

**What We Are Doing.**

We take this Incident and the security of Information in our care seriously. Upon becoming aware of the Incident, we took immediate action to contain the situation and have worked closely with data security and privacy professionals to further strengthen our existing, significant safeguards. After determining unauthorized activity had occurred, we began a thorough analysis of the information involved to identify those potentially affected and notify them.

To assist you in protecting your Information, we are offering 24 months of complimentary credit monitoring and identity theft protection services through Experian.

**What Can You Do?**

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months. While identity restoration assistance is immediately available to you, we also encourage you to activate the complimentary 24-month membership to Experian IdentityWorks and its fraud detection tools. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- You must enroll by **October 31, 2026** (Your code will not work after this date).
- Visit the Experian IdentityWorks website to enroll:**https://www.experianidworks.com/3bcredit**.
- Provide your activation code:**[insert 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 833-918-1325 by October 31, 2026. Be prepared to provide engagement number [engagement #] as proof of eligibility for the Identity Restoration services by Experian.

Although we have no evidence that an individual's personal information has been used for identity theft or fraud, it is always recommended that you remain attentive, regularly change your passwords, monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Information.

**For More Information.**

If you have any questions, you may contact us at 833-918-1325 Monday through Friday from 9 am – 9 pm Eastern Time (excluding U.S. holidays).

Sincerely,

***Travis County Credit Union***

Encl.

## ADDITIONAL RESOURCES

**Contact information for the three (3) nationwide credit reporting agencies**:

**Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com/personal/credit-report-services, 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, www.experian.com/help, 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19016, https://www.transunion.com/data-breach-help, 1-833-395-6938

**Free Credit Report.** It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Massachusetts residents**: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alert**. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

**Security Freeze.** You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting Act ("FCRA").

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. 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 Department 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, and display your name, current mailing address, and the date of issue.

**FTC and State Attorneys General Offices**. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

**Reporting of identity theft and obtaining a police report.** You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

**For California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

**For Massachusetts Residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.

**For Pennsylvania Residents**: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

**How to Apply for an IRS Identity Protection PIN**

- Go to: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.
- Select the button: "Get an IP PIN."
- The fastest way to receive an IP PIN is to request one through your ID.me account, under your "Profile" page. If you don't already have an account on IRS.gov, you must register to validate your identity.
- Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process.
- Once you have opted in and obtained an IP PIN online, you will need to retrieve your IP PIN online each calendar year as a CP01A Notice will not be mailed. The IP PIN is generally available in your online account starting in mid-January through mid-November.

If you need help applying for this PIN, please call our office.