

Colin Battersby
Direct Dial: (248) 593-2952
E-mail: cbattersby@mcdonaldhopkins.com

August 23, 2024

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Texas Dow Employees Credit Union – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents Texas Dow Employees Credit Union (“TDECU”). I am writing to provide notification of an incident at TDECU that may affect the security of personal information of approximately 229 Maryland residents. TDECU’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, TDECU do not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

TDECU was notified by a third-party vendor used by TDECU to transfer data, MOVEit, that they were compromised by a bad actor on or around May 31, 2023 in an attack that affected organizations of all kinds around the world. Certain TDECU data may have been viewed or taken by the bad actor as part of this attack.

Upon learning of this issue, TDECU immediately commenced a prompt and thorough investigation. As part of the investigation, TDECU engaged external cybersecurity professionals who regularly investigate and analyze these types of situations to help determine the extent of any compromise of the information on the TDECU network. It was determined that there was no compromise of TDECU’s broader network security. Following our investigation, we discovered on July 30, 2024, that certain files containing personal information of TDECU members were potentially removed from MOVEit by the bad actor between May 29-31, 2023. The impacted data includes full names in combination with Date of Birth, Social Security Number, Bank / Financial Account Number, Credit / Debit Card Number, Driver's License / Government ID, and Taxpayer Identification Number. Not all data elements were impacted for every Maryland resident. On August 20, 2024, TDECU located the most recent contact information for the impacted individuals.

To date, TDECU is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, TDECU is providing notice to the affected individuals commencing on August 23, 2024 in substantially the same form as the

August 23, 2024

Page 2

enclosed letter (Attached as Exhibit A). The notified individuals who have had their Social Security number impacted will receive complimentary credit monitoring services. Additionally, TDECU will advise all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. TDECU will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for TDECU. TDECU remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. TDECU continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Colin Battersby

Encl.

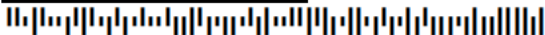
Exhibit A



YOUR CREDIT UNION

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

24 1 3845 *****AUTO**5-DIGIT 77534



***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]:

I am writing with important information regarding a recent data security incident that Texas Dow Employees Credit Union (“TDECU”) experienced. The privacy and security of the protected personal information entrusted to us is of the utmost importance to TDECU. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

A third-party vendor used by TDECU to transfer data, MOVEit, was compromised by a bad actor on or around May 31, 2023 in an attack that affected thousands of organizations, government entities, private businesses, financial institutions and more around the world, with over 20 million individuals impacted. Certain TDECU data may have been viewed or taken by the bad actor as part of this attack. There was no compromise of TDECU’s broader network security.

What We Are Doing.

Upon being informed of the vulnerability, TDECU immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third party professionals to assist in the investigation and remediation of the vulnerability. Following our investigation, we discovered on July 30, 2024, that certain files containing personal information of TDECU members were potentially removed from MOVEit by the bad actor between May 29-31, 2023. We want to make you aware of the incident and provide you with steps you can take to protect your information further.

What Information Was Involved?

The data accessed by the unauthorized actor contained your [REDACTED]

What You Can Do.

We have no evidence that any of your information has been used for identity theft or to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

We are providing you with complimentary access to Experian IdentityWorksSM for 12 months. 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).

This letter also provides other precautionary measures to protect your personal information, including placing a fraud alert and/or security freeze on your credit files and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We sincerely regret the occurrence of this incident. We have always been committed to maintaining the proper handling, protection, and privacy of protected personal information in our possession and have taken precautions to safeguard it. Though this incident did not result from a compromise of TDECU systems, we continually evaluate and modify our practices and controls to enhance the security and privacy of your personal information. MOVEit has represented that the vulnerability exploited in this attack has been fixed.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]. Representatives are available from 8:00 am to 8:00 pm Central Time, Monday through Friday, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information.

Sincerely,

TDECU — Your Credit Union
1001 FM 2004
Lake Jackson, TX 77566

– OTHER IMPORTANT INFORMATION –

1. Additional Details Regarding Your Experian IdentityWorks Membership.

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 12-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 **November 13, 2024** (*The code will not work after this date.*)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Your activation code: [REDACTED]

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 833-918-1098. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

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.
- **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.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338) or TTY: 1-866-653-4261, or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

You may also reach out to the Social Security Administration to notify them of the impact on your Social Security Number. They may be reached via the telephone by contacting the National 800 Number at 1-800-772-1213 between 8:00 a.m. – 7:00 p.m. Eastern Time, Monday through Friday. If you are deaf or hard of hearing and use TTY equipment, you can call the TTY number at 1-800-325-0778.

6. State Specific Information.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this 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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA) which 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, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.
There were 20 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.