

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

October 9, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: University Federal Credit Union – Incident Notification

Dear Mr. Brown:

McDonald Hopkins PLC represents University Federal Credit Union (“UFCU”), located at PO Box 9350, Austin, TX 78766-9350. I am writing to provide notification of an incident at UFCU that may affect the security of personal information of approximately one hundred and twelve (112) Maryland residents. UFCU’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, UFCU does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

University Federal Credit Union received notice from a third-party vendor regarding a security vulnerability in the MOVEit Transfer solution which is utilized by University Federal Credit Union. On May 31, 2023, MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on MOVEit Transfer. There was no compromise of University Federal Credit Union’s broader network security.

Upon learning of this issue, UFCU immediately commenced an internal investigation and applied all to date security patches provided by Progress Software and revised the file retention configuration. The investigation revealed that the information was likely obtained by the unauthorized individual between May 27, 2023, and May 31, 2023. Following the investigation, UFCU conducted a thorough review of the impacted data and discovered on September 15, 2023 that certain files that contain personal information were potentially removed from the network by an unauthorized party. Information potentially impacted for Maryland residents includes Social Security number, account number, routing number, financial institution name, and/or credit or debit card number. Not all information was impacted for all individuals.

UFCU wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. UFCU is providing the affected residents with written notification of this incident commencing on or about October 10, 2023 in substantially the same form as the letter attached hereto. UFCU is offering the residents whose Social Security number was impacted a complimentary one-year membership with a credit monitoring service. UFCU will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. UFCU will 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, the Federal Trade Commission, and the Maryland Attorney General Consumer Protection Division.

At UFCU, protecting the privacy of personal information is a top priority. UFCU is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. UFCU continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (248) 593-2952 or cbattersby@mcdonaldhopkins.com.

Very truly yours,



Colin M. Battersby

Encl.



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY



October 10, 2023

NOTICE OF GLOBAL DATA SECURITY EVENT

Dear [REDACTED]:

We are reaching out to let you know about a recent incident that involves the security of your personal information. This notice is being sent out of an abundance of caution, as **we have NO evidence that any of your information has been used to commit financial fraud**. However, we encourage you to read further to learn what happened and how you can protect yourself. Rest assured that we truly value our relationship and we have committed resources to make sure that this event continues to receive our highest priority.

What Happened?

On May 31, 2023, we received notice from one of our vendors, MOVEit, that they experienced a global data security event that allowed unauthorized users access to data stored on their software platform. MOVEit is a widely used file transfer software and they have publicly acknowledged the incident and provided patches to fix the problem. According to online security firm estimates, this global data security event is projected to have affected hundreds or even thousands of organizations worldwide and millions of individuals. However, there was no compromise of our UFCU network security from this event.

What We Are Doing.

Once informed, we immediately began to determine what—if any—information might have been compromised and we engaged third-party professionals to assist us in our due diligence. As part of that investigation, we learned that some UFCU files have been copied and removed from the MOVEit platform by an unauthorized party. We discovered on September 15, 2023, that the files potentially contained some of your personal information.

What Information Was Involved?

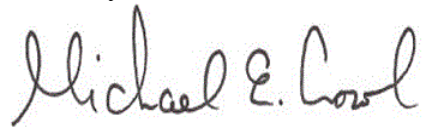
We are not currently aware of any identify theft or fraud to our Members from this incident. However, the information that was accessed could possibly contain some of your personal information, including your [REDACTED]. As a reminder, UFCU will NEVER contact you to ask for your personal information, so please do not share your personal financial information with anyone you do not know.

What You Can Do.

Again, we have NO evidence that any of your information has been used to commit financial fraud. We will continue to actively monitor this situation. However, to help ease any concerns you may have and to further protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months. Attached to this letter, you will find information on how to activate this offer, as well as how to place a fraud alert and security freeze on your credit files, and how to obtain a free credit report so that you may review any recent activity. Please remember to remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

If you have any questions, please call 866-240-5440, Monday-Friday, 8 AM – 6 PM CT. This is a dedicated and confidential toll-free number with knowledgeable representatives who are familiar with this incident and can help explain how to protect the misuse of your information. We are deeply committed to maintaining the privacy of your personal information and we have taken precautions to continue safeguarding it. We continually evaluate and modify our practices and internal controls to prioritize your privacy and security. Please reach out if we can help. Thank you for your membership and the trust that you have placed in UFCU.

Sincerely,

A handwritten signature in dark ink that reads "Michael E. Cowl". The signature is fluid and cursive, with the first letters of the first and last names being capitalized and prominent.

Michael E. Cowl
CEO & President
University Federal Credit Union

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring

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 12 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 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** [REDACTED], no later than 5:59pm CT. Your code will not work after this date
- Visit the Experian IdentityWorks website to enroll: [REDACTED]
- Provide 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 1-877-288-8057 by **12/21/2023**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR
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.
- **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 one-year “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 credit monitoring services, 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 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.

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.marylandattorneygeneral.gov, Telephone: 888-743-0023.

New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

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; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

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.

Rhode Island Residents: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may need to provide the following information: your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number; date of birth; complete address; prior addresses; proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. When you place a security freeze on your credit report, within five (5) business days you will be provided with a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number or password provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) the proper information regarding the period of time for which the report shall be available to users of the credit report. There were 11 of Rhode Island residents impacted.

