

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

September 1, 2023

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

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Space Coast Credit Union – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Space Coast Credit Union (“SCCU”) of Melbourne, Florida. I am writing to provide notification of an incident that may affect the security of personal information of approximately one (1) Maryland resident. By providing this notice, SCCU does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

SCCU received notice from one of our third-party vendors regarding a security vulnerability in the MOVEit Transfer solution which is utilized by SCCU. Upon learning of the issue, SCCU contained the incident through patches and commenced a prompt and thorough investigation in consultation with external forensic investigators and data privacy professionals.

After an extensive investigation, SCCU discovered on August 2, 2023 that the MOVEit database which was accessed on or about May 30, 2023, contained personal information pertaining to the Maryland resident, such as name, date of birth, Social Security number, drivers license, and financial account information.

SCCU is providing the affected resident with written notification of this incident commencing on or about September 1, 2023 in substantially the same form as the letter attached hereto. SCCU will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. The affected resident will also be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission, in addition to credit monitoring services.

At SCCU, protecting the privacy of personal information is a top priority. SCCU is committed to maintaining the privacy of personal and financial information in its possession and has taken many precautions to safeguard it.

September 1, 2023

Page 2

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

Encl.



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

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

RE: NOTICE OF DATA SECURITY EVENT

Dear <<first_name>>:

The privacy and security of the personal information entrusted to us is of the utmost importance to Space Coast Credit Union ("SCCU"). We are writing to provide you with information regarding a recent third-party data incident which involves the security of some of your personal information that was supplied to us. 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 help protect your information.

What Happened?

Space Coast Credit Union received notice from one of our third-party vendors regarding a security vulnerability in the MOVEit Transfer solution which is utilized by SCCU. MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on the MOVEit server. MOVEit has acknowledged the vulnerability and has since provided patches to remediate the exploit. There was no compromise of Space Coast Credit Union's broader network security.

What We Are Doing

Upon being informed of the vulnerability, Space Coast Credit Union 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 August 2, 2023 that certain files that contain your personal information were potentially removed from our network by an unauthorized party on May 30, 2023. To date, Space Coast Credit Union is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident.

What Information Was Involved?

The information potentially accessible on the MOVEit server could have included your <<b2b_text_1(name, data elements)>>.

What You Can Do

We have no evidence that any of your information has been used to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. We are also offering a 12 month complimentary membership of Experian IdentityWorksSM Credit 1B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft.

IdentityWorks Credit 1B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 1B, including instructions on how to activate your complimentary membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to help protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and 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

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information, including a review of our ongoing third-party vendor relationships.

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 [TFN](#). This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

Space Coast Credit Union

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12 months Credit Monitoring**

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

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** <<b2b_text_6(enrollment deadline)>> (Your code will not work after this date.)

Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>

Provide your **activation code**: <<activation code s_n>>

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 <<b2b_text_6(enrollment deadline)>>. Be prepared to provide engagement number <<b2b_text_2(engagement number)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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, 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.

2. **Placing a Fraud Alert.**

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial one (1) 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’ll 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 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.

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.

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.

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.