

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

December 6, 2023

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

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

Re: WEOKIE Federal Credit Union – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents WEOKIE Federal Credit Union (“WEOKIE”). I am writing to provide notification of an incident at WEOKIE that may affect the security of personal information of Maryland residents. By providing this notice, WEOKIE does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

WEOKIE received notice from one of our service providers regarding a security vulnerability in the MOVEit Transfer solution, which is utilized by our service provider. Between May 27 and May 31, 2023, unauthorized individuals obtained files containing certain personal information from a widely used file transfer service called MOVEit Transfer. Thousands of organizations around the world, including one of WEOKIE’s service providers, use MOVEit Transfer to move sensitive data. There was no compromise of WEOKIE’s broader network security. On or about October 19, 2023, WEOKIE was notified by our service provider, Fiserv, that Maryland resident information was impacted. After an extensive review, WEOKIE discovered that certain personal information of approximately one (1) Maryland resident was included within the files that were subject to unauthorized access or acquisition as a result of the incident. The personal information contained within the impacted data included first and last name, account number, and/or routing number.

WEOKIE has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, WEOKIE 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. WEOKIE is providing the affected residents with notification of this incident, commencing on or about December 6, 2023. The notice will be in substantially the same form as the letter attached hereto. WEOKIE is also offering the affected residents whose Social Security number was potentially impacted by the incident with complimentary two-year

membership with a credit monitoring service. WEOKIE is advising the affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. WEOKIE is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

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

Sincerely,



Dominic A. Paluzzi

Encl.

NOTICE OF DATA BREACH

Dear [REDACTED]

What Happened?

You may be aware of the cybersecurity event that is impacting thousands of organizations across the world involving a software product called MOVEit. MOVEit Transfer by Progress Software is a commonly used secure Managed File Transfer (MFT) software supporting file transfers. The event involving MOVEit Transfer has resulted in the potential exposure of personal data for millions of individuals around the world. MOVEit Transfer is used by government agencies, financial firms, universities, and other well-respected organizations. The MOVEit Transfer software was used to support some of our institution's services. On [REDACTED] we learned that personal information related to our institution was involved in the incident.

On May 31, 2023, Progress Software, the owner of MOVEit, announced a previously unknown vulnerability in its MOVEit Transfer application. That vulnerability, which allowed unauthorized actors to defeat MOVEit's security measures, was exploited and resulted in the potential exposure of sensitive information for any organization utilizing the software.

Analysis to date has identified unauthorized activity in the relevant MOVEit Transfer environment between May 27 to 31, 2023, which was before Progress Software publicly disclosed the existence of this vulnerability. During that time, unauthorized actors obtained files transferred via MOVEit Transfer which included certain personal information.

What Information Was Involved?

From a careful review of the contents of the files, we have determined that one or more of the files may have contained information including [REDACTED]

While the MOVEit incident did not impact WEOKIE's computers or operating systems, we are notifying all individuals who were affected by this incident.

Through the investigation, WEOKIE determined that unauthorized actors exploited the then-unknown MOVEit vulnerability to download a data file that contained certain personally identifiable information about some of our members. This file may have contained [REDACTED]

What We Are Doing.

We wanted to notify you of this incident and assure you that we take it seriously. Upon learning of the incident, WEOKIE immediately activated its incident response procedures and launched a thorough investigation to determine the extent of the impact and identify potentially impacted individuals. WEOKIE retained outside advisors and cybersecurity experts to assist in its evaluation of the situation. To help prevent something like this from happening again, our service provider has remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Our service provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities.

What You Can Do.

At this time, WEOKIE is not aware of any reports of identity fraud or improper use of information pertaining to your WEOKIE account as a direct result of this incident. For members affected, we have arranged for you to receive a complimentary free identity monitoring service through Kroll for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained unintentional exposure to confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

For more information on identity theft prevention, including instructions on how to activate your identity monitoring, as well as some additional steps you can take for your protection, please review Attachments A and B that follow this letter.

Regardless of whether you elect to activate the identity monitoring service, we strongly encourage all members to take proactive steps to protect their information, including:

- Monitor your financial account activity and statements regularly to protect yourself from fraud, identity theft, and unauthorized use of your account. Notify us or any other of your financial institutions if you suspect any unauthorized activity.
- Visit AnnualCreditReport.com or call 877-322-8228 to secure a free copy of your credit report.
- Consider placing fraud alerts or credit freezes with the three credit reporting agencies.
- Equifax: 800-349-9960 or visit their website at <https://www.equifax.com>.
- Experian: 888-397-3742 or visit their website at <https://www.experian.com/>
- TransUnion: 888-909-8872 or <https://www.transunion.com/>
- Be alert to phishing attempts via email, phone calls, or text messages from potential scammers asking for personal or financial information.

For More Information.

Please be assured that we are taking steps to address the incident and to help protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact us at [REDACTED]

Sincerely,

[REDACTED]

ATTACHMENT A

Visit [REDACTED] to activate and take advantage of your identity monitoring services.

You have until [REDACTED] to activate your identity monitoring services.

Membership Number: [REDACTED]

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



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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help 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.

ATTACHMENT B

ADDITIONAL STEPS YOU CAN TAKE

To help protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:

Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to help protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

District of Columbia Residents: The Attorney General can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or <https://oag.dc.gov/>.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

Massachusetts Residents: 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.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or <http://www.ncdoj.gov>.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Avenue, Albany, NY, 12231-001, (518) 474-8583/(800) 697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY, 12224-0341, (800) 771-7755, <https://ag.ny.gov>.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or <http://www.riag.ri.gov/>. You may also file a police report by contacting local or state law enforcement agencies.