

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

June 1, 2023

Via E-Mail (IDTheft@oag.state.md.us)

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

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Diamond Lakes Federal Credit Union ("Diamond Lakes") located at PO Box 1080, Malvern, Arkansas 72104 and write to inform you of a data security incident. By providing this notice, Diamond Lakes does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On December 6, 2022, Diamond Lakes discovered suspicious activity related to one employee email account. Upon discovery, Diamond Lakes took swift action to secure its email system and network. Diamond Lakes immediately launched an internal investigation and engaged leading, independent cybersecurity specialists to investigate the full scope of this incident. Based on the investigation, Diamond Lakes confirmed that one employee email account was subject to unauthorized access from December 1, 2022 to December 6, 2022. In addition to the employee email account, the forensic investigation revealed that certain network files were also subject to unauthorized access. Diamond Lakes immediately began a thorough review of the contents of the email account and the files to determine the type of information contained within and to whom that information related. Diamond Lakes also underwent a comprehensive review of its internal files in order to obtain sufficient address information to provide notification to the potentially impacted individuals.

The review of the potentially affected files was completed on January 4, 2023. While the review of the contents of the email account was still ongoing, Diamond Lakes provided notice to those with information contained within the potentially affected files on January 30, 2023. There were no Maryland residents in this initial population.

The review of the contents of the email account was completed on May 5, 2023. At that time, it was determined that information related to 11 Maryland residents was potentially subject to unauthorized access. The information believed to potentially be at risk includes a first and last name, in combination with a Social Security number, driver's license number, financial account number and/or routing number.

On May 31, 2023, Diamond Lakes sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Very truly yours,



Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-888-220-5226
Or Visit:
<https://response.idx.us/DLFCU>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

May 31, 2023

<<Notice of Data Breach>>

Dear <<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>:

We are writing to inform you of a data security incident experienced by Diamond Lakes Federal Credit Union ("Diamond Lakes") that may have involved your information as described below. We take the privacy and security of all information very seriously, and while we have no evidence to suggest that any information was subject to actual or attempted misuse, this letter includes information about the incident, our response, and steps you can take to help protect your information.

What Happened: On December 6, 2022, we discovered suspicious activity related to one employee email account. Upon discovery, we took swift action to secure our email system and network. We also launched an internal investigation and engaged leading, independent cybersecurity specialists to investigate the full scope of this incident. Based on the investigation, we confirmed that one employee email account was subject to unauthorized access from December 1, 2022 to December 6, 2022. In addition to the employee email account, the forensic investigation revealed that certain files were also subject to unauthorized access. We immediately began a thorough review of the contents of the email account and the files to determine the type of information contained within and to whom that information related. Our review of the potentially affected files was completed on January 4, 2023. While the review of the contents of the email account was still ongoing, we provided notice to those with information contained within the potentially affected files on January 30, 2023. Our review of the contents of the email account was completed on May 5, 2023. We are now notifying those individuals whose information was contained within the affected email account and, therefore, are potentially impacted by this incident.

What Information Was Involved: The information believed to be potentially at risk includes your first and last name, in combination with your <<Data Elements>>.

What We Are Doing: We have taken every step necessary to address the incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately took the steps described above, including performing password resets. We have also implemented additional technical safeguards to further enhance the security of information in our possession and prevent similar incidents from happening in the future. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, an online credit monitoring service for <<12/24>> months provided by IDX. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

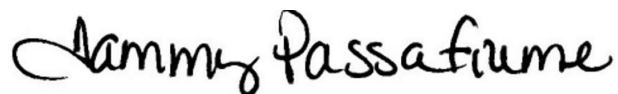
What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can

enroll to receive the complimentary credit monitoring service we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at 1-888-220-5226 Monday through Friday from 8 a.m. to 8 p.m. Central Standard Time.

The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

A handwritten signature in black ink that reads "Tammy Passafiume". The signature is written in a cursive, flowing style.

Tammy Passafiume
President & CEO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

1. Website and Enrollment. Go to <https://response.idx.us/DLFCU> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 31, 2023.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-888-220-5226 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and

7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag@dc.gov. Diamond Lakes Federal Credit Union may be contacted at PO Box 1080, Malvern, Arkansas 72104.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Diamond Lakes Federal Credit Union may be contacted at PO Box 1080, Malvern, Arkansas 72104.

For 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 bureaus 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 reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.