MAYNARDNEXSEN

RECEIVED

JAN 22 2024

CONSUMER PROTECTION

January 17, 2024

Attorney General John Formella
Consumer Protection Bureau, Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Vendor Security Incident

Dear Attorney General Formella,

Pursuant to N.H. Rev. Stat. Ann. § 359-C:20, I am writing to report a security incident on behalf of our client, Sharonview Federal Credit Union ("Sharonview"), relating to one of its vendors, Darling Consulting Group, LLC ("DCG").

DCG is a vendor utilized by Sharonview to provide financial analytics services. On May 31, 2023, Progress Software, the maker of the widely used managed file transfer software MOVEit Transfer, issued an alert regarding a zero-day vulnerability within MOVEit Transfer. Sharonview does **not** itself use MOVEit Transfer. However, on August 1, 2023, DCG reported to Sharonview that the zero-day MOVEit Transfer vulnerability had been successfully exploited on May 30-31, 2023, to obtain unauthorized access to a DCG server storing files that referenced the personal information of some Sharonview customers, including their

.

Sharonview promptly began an assessment of the files to identify the names of individuals whose information was contained within the affected records. Notices to individuals, including one (1) New Hampshire resident, began mailing on December 4, 2023 at the conclusion of data mining. Sharonview is not aware of any actual or attempted misuse of personal information as a result of this incident. However, individuals were offered complimentary credit monitoring and identity restoration services for . A copy of the individual notice is enclosed.

As part of its ongoing commitment to maintain the security of its customers' information, Sharonview is reviewing existing policies and procedures that govern third party vendors and evaluating additional measures and safeguards for third parties that store personal information on Sharonview customers.

Please do not hesitate to let me know if you have any questions.

Very truly yours,

Todd Panciera, Jr.

Enclosure

Sharonview Federal Credit Union
c/o Cyberscout
<Return Address>
<City> <State> <Zip>

SHARONVIEW®
FEDERAL CREDIT UNION

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

<<Date>>

NOTICE OF SECURITY INCIDENT

Dear <<FirstName>>,

Sharonview Federal Credit Union recently became aware of a potential security incident with Darla Consulting Group (DCG) that may have affected your personal information. DCG provides financial analytics services to Sharonview. We are providing this notice as a precaution to let you know about the incident and to call your attention to some steps you can take to protect yourself. We sincerely regret any concern this may cause you.

What Happened?

On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software, disclosed a vulnerability in their software that could be exploited by an unauthorized third party. DCG utilizes MOVEit in their regular course of their business operations to securely transfer files. DCG launched an investigation and determined that between May 30, 2023, and May 31, 2023, unauthorized access to DCG's network occurred as a result of the MOVEit vulnerability. Data files that Sharonview provides to DCG for analysis were potentially exposed as a result.

You are receiving this letter because your personal information was included in the files exposed by this incident. At this time, we have no evidence that your personal information has been misused as a result of this incident. However, we are providing this notice because we cannot establish with certainty that such access did not or will not occur.

What Information Was Involved?

The personal information involved includes your .

What We Are Doing

As soon as DCG identified this issue, DCG immediately removed access and blocked any further attempts to access this information.

What You Can Do

We are committed to helping our members who may have been impacted by this unfortunate situation. In response to the incident, we are providing you with access to the following services:

Additionally, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring** services at no charge. These services provide you with alerts for from the date of enrollment when changes occur to

your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://www.xxxx.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<Unique Code>>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Credit Monitoring services require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We recommend that you monitor your accounts, review account statements closely, and monitor your credit report for unusual activity or indications of identity theft over the next 12 to 24 months, and promptly notify us to report incidents of suspected identity theft. Additionally, we are including with this letter an attachment listing additional recommended steps you may wish to consider.

For More Information

We take the security of your information very seriously, and we regret any inconvenience or concern this incident may cause you. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. If you have questions, please call the help line at 1-800-XXX-XXXX and supply the fraud specialist with your unique code listed above.

Sincerely,

Sharonview

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Review Your Account Statements and Credit Reports. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely.

If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/ or the Federal Trade Commission ("FTC").

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call the toll-free number 877-IDTHEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www. annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, PO Box 105281, Atlanta, GA 30348. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies, whose contact information is listed below.

Equifax	Experian	TransUnion
800-685-1111 www.equifax.com PO Box 740241 Atlanta, GA 30374	888-397-3742 www.experian.com/fraud 475 Anton Blvd. Costa Mesa, CA 92626	800-888-4213 www.transunion.com/fraud 2 Baldwin Place, PO Box 1000 Chester, PA 19022

Fraud Alert. There are also two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. An initial fraud alert on your credit report is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies listed above.

Credit Freeze. You have the right to place a credit freeze, also known as a security freeze, on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential creditors from accessing your credit report without your consent. If you place a freeze, potential creditors will not be able to access your credit report without your consent unless you temporarily lift the freeze. Consequently, placing a credit freeze may interfere with or delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency. To find out more on how to place a security freeze, you can use the following contact information:

Equifax	Experian Security Freeze	TransUnion
P.O. Box 105788 Atlanta, GA 30348 800-685-1111 www.equifax.com/help/credit-freeze/en_cp	P.O. Box 9554 Allen, TX 75013 888-397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19022-2000 888-909-8872 www.transunion.com/securityfreeze

You can obtain information more information about fraud alerts and credit freezes from the FTC or any of the three credit reporting agencies.

Additional Free Resources on Identity Theft

The FTC provides tips on how to avoid identity theft. For more information, please visit www.ftc.gov/idtheft; call 1-877-ID-THEFT (1-877-438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

ADDITIONAL INFORMATION FOR RESIDENTS OF CERTAIN STATES

If you are a North Carolina resident, for more information about preventing identity theft, you may contact the North Carolina Attorney General office at 9001 Mail Service Center, Raleigh, NC 27699-9001, or by calling 919-716-6400, or visit the Attorney General website at http://www.ncdoj.com/.

If you are a South Carolina resident, effective January 1, 2015, an amendment to the South Carolina Consumer Protection Code allows parents, guardians, and representatives to create and freeze a protected consumer's credit file for free. A protected consumer is someone under the age of 16 or an incapacitated adult who does not currently have a credit report. Upon receiving a request on behalf of a protected consumer, the credit reporting agency will create a credit file in that protected consumer's name and freeze it, helping to deter identity theft. Parents/guardians must contact each credit reporting agency to place this freeze. There is no charge to place a protected consumer freeze. For more information about security freezes, contact the Department of Consumer Affairs or visit www.consumer.sc.gov.

If you are a California resident, for more information on identify theft, you may visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov.

If you are a resident of the District of Columbia, you can contact the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, by calling 202-442-9828, or by visiting https://oag.dc.gov/consumer-protection.

If you are a New York resident, you can contact the Office of the Attorney General, Bureau of Consumer Frauds & Protection, by calling 800-771-7755.