

November 30, 2023

VIA WEBSITE PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Frey

Constangy, Brooks, Smith & Prophete, LLP represents Broadview Federal Credit Union (“Broadview”), a federally chartered credit union serving New York state, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine’s data breach notification statute.

Nature of the Security Incident

On November 3, 2023, one of Broadview’s external vendors, Fiserv, notified Broadview that it was one of many organizations across the globe that was affected by the MOVEit Transfer software vulnerability. MOVEit Transfer by Progress Software Corp. is a tool used by organizations to transfer files. On May 31, 2023, and again in June 2023, Progress Software Corp. publicly disclosed zero-day vulnerabilities that impacted the MOVEit Transfer tool. These vulnerabilities permitted an unauthorized actor to download files from Fiserv that contained individuals’ personal information.

Fiserv notified Broadview that files were downloaded from Fiserv’s MOVEit environment by the unauthorized actor between May 27 and 31, 2023, and that the downloaded files included personal information of Broadview members. As soon as Broadview received this notification from Fiserv, Broadview took steps to review and understand what data was impacted. Based on the review of impacted data, personal information may have been impacted by this incident.

The information affected may have included name, Broadview account number, and routing number.

Number of Maine Residents Involved

On November 30, 2023, Broadview notified 5 Maine residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, Broadview is providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering individuals complimentary identity protection services through IDX. These services include 24 months of credit and Cyberscan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

Broadview has also established a toll-free call center through IDX to answer questions about the incident and address related concerns.

Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at LNickle@Constangy.com.

Sincerely,



Lindsay B. Nickle
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter



4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

Enrollment Code: <<XXXXXXXXXX>>
To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/broadviewfcu>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 30, 2023

Subject: Notice of Data <<Variable 1>>

Dear <<First Name>> <<Last Name>>:

I am writing to notify you of a cybersecurity incident at one of our external vendors that may have included your personal information. We take the privacy and security of personal information very seriously and we encourage you to review this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Information Was Involved. The potentially affected information may have included your name, address, and Broadview account number. This is the same information that is found on your checks.

What Information Was NOT Involved. Personal information such as your social security number, date of birth, government-issued ID information, credit score, account balances, or any other sensitive information.

What Happened. One of our vendors, Fiserv, notified us that they were one of many organizations across the globe that was affected by the MOVEit Transfer software vulnerability. MOVEit Transfer by Progress Software Corp. is a tool used by organizations to transfer files. On May 31, 2023, and again in June 2023, Progress Software Corp. publicly disclosed vulnerabilities that impacted the MOVEit Transfer tool. These vulnerabilities permitted an unauthorized actor to download files from Fiserv that contained individuals' personal information.

On November 3, 2023, Fiserv notified Broadview that files were downloaded from Fiserv's MOVEit servers by the unauthorized actor between May 27 and 31, 2023. The downloaded files included the personal information of a very limited number of Broadview members. As soon as we received this notification from Fiserv, we took steps to review what data was impacted. Your personal information may have been part of this incident. We reviewed all impacted accounts and have **no evidence** of any unauthorized access to any Broadview account. **Please note that none of Broadview's banking systems were accessed or compromised as a result of this incident.**

What We Are Doing. Fiserv has confirmed that it has remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Broadview will continue to monitor potentially affected accounts for suspicious activity.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

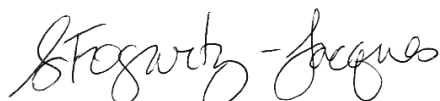
What You Can Do: Please review the guidance included with this letter about additional steps you can take to protect your information. Also, we encourage you to contact IDX with any questions and to enroll in the free identity protection

services by calling 1-888-998-6645, going to <https://response.idx.us/broadviewfcu>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 29, 2024. Please do not discard this letter, as you will need the Membership Number provided above to access services.

For More Information. Please call 1-888-998-6645 or go to <https://response.idx.us/broadviewfcu> for assistance or for any additional questions you may have.

We regret any inconvenience this may cause you and encourage you to take advantage of the credit monitoring services offered. Please be assured that the confidentiality of your personal information is of utmost importance to us. We take your trust in us and this matter very seriously.

Sincerely,

A handwritten signature in cursive script that reads "S. Fogarty-Jacques".

Susan Fogarty-Jacques
Chief Experience Officer
Broadview Federal Credit Union
4 Winners Circle
Albany, NY 12205

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: 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).

Copy of Credit Report: 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 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.