

EXHIBIT 1

We continue to represent Bradford-Scott Data, LLC (“Bradford-Scott”) and provide this supplemental notice on behalf of Community Credit Union of New Milford, Inc. regarding an additional seven (7) Maine residents impacted by the event first reported to your office on February 29, 2024.

Bradford-Scott continues its efforts to provide notification to individuals on behalf of data owners on a rolling basis. As such, this notice may be further supplemented as this effort continues and until Bradford-Scott completes the individual notifications. By providing this notice, Bradford-Scott does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Notice to Maine Residents

On or about February 13, 2024, Bradford-Scott began providing written notice of this event to impacted individuals. On or about March 12, 2024, Bradford-Scott will be providing an additional set of written notices regarding this event, which includes seven (7) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

The personal information present in the relevant files may include name and Social Security number.


EXHIBIT A




4145 SW Watson Ave.
Suite 400
Beaverton, OR 97005

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

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





Or Visit:
<https://app.idx.us/account-creation/protect>

March 12, 2024

<<Variable 2>>

Dear <<Name 1>> <<Name 2>>:

Bradford-Scott Data, LLC (“Bradford-Scott”) is writing to provide you with notice of a data security event that may impact the privacy of your information provided to Bradford-Scott as a technology and service provider of <<Variable Data 3>>. This letter contains information about the event, our response, and steps you can take to better protect your information, should you feel it appropriate to do so.

What Happened? On July 2, 2023, we identified unusual activity within a limited portion of our network. In response, we immediately took steps to ensure the security of our environment and initiated an investigation to determine the full nature and scope of the activity. Through this investigation, we learned that certain files were likely copied from our network between May 19 and May 28, 2023. We then began a time-intensive and detailed review of all files determined to be affected by this event to determine what information was present in the files and to whom it related. You are receiving this letter because we determined after the detailed data review was complete on or about December 10, 2023, that your information was present in the potentially affected files. We have seen no evidence to date of any fraudulent use of any data as a result of this event.

What Information Was Involved? Based on our review, we determined that the personal information present in the potentially affected files includes your name, and <<variable data 4>>.

What We Are Doing. Bradford-Scott takes this event and the privacy of information in our care seriously. Upon discovery of the event, we conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of our network environment, conducted a comprehensive review of the information potentially affected, and reported this event to federal law enforcement. Further, as part of our ongoing commitment to the privacy and security of information in our care, we implemented multiple additional security measures and safeguards to further enhance our existing policies and processes.

In addition to notifying you, we will be notifying applicable state and federal regulators as well as the consumer reporting agencies.

As an added precaution, we are providing you with access to credit monitoring services for <<12/24>> months at no cost to you. Information on these services and instructions on how to activate them may be found in the enclosed *Steps You Can Take to Protect Personal Information*.

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: <<12/24>> 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. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your accounts and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. We also encourage you to review the enclosed *Steps You Can Take to Protect Personal Information*.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact our dedicated assistance line at 1-888-466-5849, Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

We regret any inconvenience caused by this event and remain committed to safeguarding the information in our care.

Sincerely,
Bradford-Scott Data, LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note that the enrollment deadline is June 12, 2024.

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 1-888-466-5849 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If a consumer is the victim of identity theft, he or she is entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 of identity theft. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. 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 Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 24 Rhode Island residents that may be impacted by this event.