COOPER
CARGILL
CHANT
ATTORNEYS AT LAW

October 31, 2023

Attorney General John Formella
NH Department of Justice
1 Granite Place South
Concord, NH 03301

Re: RSA 359-C:20 Notification of Data Security Incident at Tri-County Community Action Program ("TCCAP")
Date of Breach: 10/23/2023
Our File #: 16553.024

Dear Attorney General Formella:

This office represents TCCAP, a NH non-profit that administers both federal and state grant programs to combat poverty in northern NH. Last week, TCCAP conducted an investigation that discovered that on or about October 23, 2023, a former employee copied and downloaded the confidential client data for approximately 944 client families, with approximately 1,486 household members identified by name. This data includes

The information downloaded in the data breach is relevant to the regulatory authority of: New Hampshire Health and Human Services Department, New Hampshire Housing Finance Authority, New Hampshire Department of Safety, GOFERR, and the New Hampshire Department of Justice. TCCAP has also contacted law enforcement and will cooperate in any further investigation of this incident.

Our investigation is ongoing. This notice is provided pursuant to RSA 359-C:20. TCCAP anticipates that written notice of this incident will be provided to all affected individuals within ten days of this letter, on or before November 9, 2023.

Should any person or entity have questions regarding this notification, or the data security event itself, please contact me at or at the addresses listed below.

Very truly yours,

COOPER CARGILL CHANT, P.A.

Christopher T. Meier
cmeier@coopercargillchant.com

CTM/kjt
cc: Client

November 9, 2023

TO THE CLIENTS OF TRI-COUNTY COMMUNITY ACTION PROGRAM

Re: Data Security Incident at Tri-County Community Action Program ("TCCAP")
Date of Breach: 10/23/2023

Dear Client:

We are writing to inform you of a recent Data Security Incident that may have involved your personal information. At TCCAP, we take the privacy and security of all of the information within our possession very seriously.

What Happened? TCCAP has discovered that on or about October 23, 2023, a former employee copied and downloaded confidential client data from TCCAP servers to their personal account, without authorization or valid purpose. Upon discovery of the incident, we took steps to secure our digital environment, and engaged IT professionals to investigate the Incident and the extent of the breach, and determine the likelihood that any data would be misused. We also have notified law enforcement of the Incident; and have taken steps to stop the further dissemination of the data.

What Information Was Involved? The Incident involved data which included

.

The data downloaded in the Incident is potentially relevant to the regulatory authority of, and/or the data of: New Hampshire Health and Human Services Department, New Hampshire Housing Finance Authority, New Hampshire Department of Safety, GOFERR, and the New Hampshire Department of Justice. This Notice is jointly made with these New Hampshire Housing Finance Authority, and contact information is below. You may contact us, or the specific agency to which your data is related, if you have questions or concerns.

What We Are Doing? As soon as we discovered the incident, we took the steps referenced above, and continued to take steps to ensure that no further dissemination of the data occurs. We have notified law enforcement, including the Federal Bureau of Investigation, and will provide whatever cooperation is necessary to hold the perpetrator(s) accountable. We continue to take steps to ensure that there is no further dissemination of the data, and prevent any misuse of the data.

Additional Steps You Can Take. Attached to this letter are two pages of additional information regarding how you can take additional steps to protect your information and protect against misuse of your personal data.

For More Specific Information. If you have any questions about this letter or the data security incident, you may contact any and all of the following, Monday through Friday from 9am to 5pm.

Sincerely,

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 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 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert 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 and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving

your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.