Donna Maddux, Partner
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, OR 97035
dmaddux@constangy.com
Direct: 503.312.6251

August 23, 2023

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

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP represents CLEAResult Consulting, Inc. ("CLEAResult"), in conjunction with a recent data security incident described in greater detail below. CLEAResult is a provider of energy efficiency, energy transition, and decarbonization solutions, headquartered in Austin, Texas. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification law.

1. Nature of the Security Incident

On May 31, 2023, Progress Software Corporation ("Progress") disclosed to all customers, including CLEAResult, that a Progress-owned transfer software tool, MOVEit Transfer, experienced a vulnerability which allowed unauthorized access to the MOVEit Transfer application ("MOVEit Incident"). CLEAResult used MOVEit to transfer files. CLEAResult is one of thousands of organizations worldwide recently affected by the MOVEit Incident.

Upon receiving notice of the MOVEit Incident, CLEAResult immediately took steps to secure its MOVEit application. CLEAResult also undertook an investigation with the assistance of external experts to confirm the scope of any potentially affected data. The investigation revealed that an unauthorized actor transferred copies of certain files from the CLEAResult MOVEit system on or about May 30, 2023. The investigation into the scope of the impact and the information affected is ongoing.

On August 4, 2023, CLEAResult determined that certain personal information was involved in the incident and is working diligently to notify these individuals.

2. Type of Information and Number of Maine Residents Affected

CLEAResult is notifying seven (7) residents of Maine of this data security incident via first class U.S. mail on August 23, 2023. The information accessed and potentially acquired by the unauthorized actor responsible for this incident may have included name, Social Security number, financial account information, and taxpayer identification number. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

CLEAResult reported this incident to the Federal Bureau of Investigation's Internet Crime Complaint Center and will cooperate with any investigative efforts in an attempt to hold the perpetrator(s) of this incident responsible, if possible. CLEAResult has also implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, CLEAResult has offered all individuals whose information was involved 24 months of complimentary services through IDX, which includes credit monitoring, dark web monitoring, a $1 million identity fraud loss reimbursement policy, fully-managed identity theft recovery services, and 90 days access to a call center.

4. Contact Information

CLEAResult remains dedicated to protecting the personal information in its possession. Should you have any questions or need additional information, please do not hesitate to contact me at 503.312.6251 or by e-mail at dmaddux@constangy.com.

Best regards,

/s/ Donna Maddux

Donna Maddux
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

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

To Enroll, Please Call:
1-888-590-5002
Or Visit:
https://response.idx.us/CLEAResult
Enrollment Code: <<Enrollment Code>>

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

August 23, 2023

Subject: Notice of Data <<Variable Text 1: Security Incident/Breach>>

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

CLEAResult, an energy efficiency and solar program administrator, is writing to inform you of a recent data security incident involving your personal information. CLEAResult collected and maintains your personal information as the administrator for the Eversource <<Variable 2:[Solar Massachusetts Renewable Target ("SMART") Program] or [Residential Renewable Energy Solutions ("RRES") Program]>>. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information. CLEAResult is also offering you the opportunity to enroll in twenty-four (24) months of identity protection services provided through IDX, at no cost to you. Activation instructions and additional information regarding the services are provided in this letter.

What Happened? On May 31, 2023, Progress Software Corporation ("Progress") disclosed to all customers, including CLEAResult, that a Progress-owned transfer software tool, MOVEit Transfer, experienced a vulnerability which allowed unauthorized access to the MOVEit Transfer application ("MOVEit Incident"). CLEAResult used MOVEit to transfer files. CLEAResult is one of thousands of organizations worldwide recently affected by the MOVEit Incident.

Upon receiving notice of the MOVEit Incident, CLEAResult immediately took steps to secure its MOVEit application. CLEAResult also undertook an investigation with the assistance of external experts to confirm the scope of any potentially affected data. The investigation revealed that an unauthorized actor transferred copies of certain files from the CLEAResult MOVEit system on or about May 30, 2023. The investigation into the scope of the impact and the information affected is ongoing.

On August 4, 2023, we determined that certain personal data relating to the <<Variable 3:SMART/RRES>> Program, including your data, was acquired as part of this MOVEit Incident.

What Information Was Involved? The impacted information may have included your name, address, phone number, email, <<Variable 4:financial account information/taxpayer identification number/social security number>> and solar project and utility account information.

What We Are Doing. As soon as we were notified of the MOVEit Incident, we took the steps described above and implemented additional security measures to help reduce the risk of a similar incident occurring in the future. We reported this incident to federal law enforcement and will cooperate with any investigative requests. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, we are offering you the opportunity to enroll in complimentary identity protection services through IDX – a data breach and recovery services expert. These services include 24 months of credit monitoring and CyberScan

monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. CLEAResult recommends that you review the guidance included with this letter about how to protect your information. We also encourage you to enroll in the complimentary credit monitoring and identity monitoring services, which are free to you upon enrollment.

You can enroll in the IDX identity protection services by calling 1-888-590-5002 or going to https://response.idx.us/CLEAResult and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6:00 a.m. to 6:00 p.m. Eastern Time. You will need to reference the enrollment code in this letter when calling or enrolling online, so please do not discard this letter. Please note the deadline to enroll is November 23, 2023.

For More Information: Further information about how to help protect your information appears on the following page. If you need assistance enrolling in the complimentary services being offered to you, please call IDX at 1-888-590-5002 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). IDX representatives can also answer questions you may have regarding the incident and the protection of your personal information.

We take this event and the security of information in our care seriously. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Divakar Jandhyala
Chief Product & Technology Officer
CLEAResult
2000 SW First Ave, Suite 220
Portland, OR 97201

STEPS YOU CAN TAKE TO HELP 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.

Additional Information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov; https://oag.dc.gov/

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; https://www.marylandattorneygeneral.gov/

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; https://ncdoj.gov/

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Rhode Island: The total number of individuals receiving notification of this incident is 10. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov; https://ago.vermont.gov/