Maria Efaplomatidis, Partner
Cybersecurity & Data Privacy Team
45 Main Street Suite 206
Brooklyn, NY 11201
mefaplomatidis@constangy.com
718.719.6475

January 17, 2026

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith, & Prophete, LLP represents Daniel H. Cook Associates ("DHCA") 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, Me. Rev. Stat. tit. 10 § 1348. DHCA hereby reserves all rights and defenses in connection herewith.

1. Nature of the Security Incident

On October 17, 2025, DHCA experienced a network disruption and immediately initiated an investigation into the matter. DHCA engaged cybersecurity experts to assist with the process. Following a comprehensive review of the potentially impacted data, DHCA determined that some of your residents' personal information may have been impacted in connection with this incident which is the reason for this notification. At this time, DHCA is not aware of any misuse of any information as a result of this incident.

The potentially affected information varies for each individual but may have included individuals' names and Social Security number.

2. Number of Maine Residents Affected

On January 16, 2026, DHCA notified approximately two Maine residents within the potentially affected population via USPS First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as DHCA learned of the unusual network activity, it took steps to secure its systems and launched an investigation to learn more about what happened and what information could have

been affected. DHCA implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

DHCA is also offering affected individuals with 12 months of complimentary credit monitoring and identity protection services through Epiq - Privacy Solutions ID. These services include Single Bureau Credit Monitoring with Alerts, Social Security number and Dark Web Monitoring, Identity Restoration and Lost Wallet Assistance, and a $1M Identity Theft Insurance policy. In addition, DHCA has established a toll-free call center through IDX to answer questions about the incident and address related concerns.

Additionally, DHCA is providing impacted individuals with guidance on how to better protect against identity theft and fraud. DHCA is also providing individuals with information on how to place a fraud alert and security freeze on their credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at mefaplomatidis@constangy.com or 718.719.6475

Sincerely,

Maria Efaplomatidis
Partner, Constangy Cyber Team

Encl: Sample Notification Letter

Daniel H. Cook Associates, Inc.
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<ENROLLMENT>>
Enrollment Deadline: April 16, 2026

To Enroll, Scan the QR Code Below:

SCAN ME

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

January 16, 2026

Subject: Notice of Data <<Variable Data 2: Security Incident / Breach>>

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

We are writing to inform you of a recent data security incident experienced by Daniel H. Cook Associates, Inc. ("DHCA") that may have involved your personal information. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On October 17, 2025, DHCA experienced a network disruption and immediately initiated an investigation of the matter. DHCA engaged cybersecurity experts to assist with the process. As a result of the investigation, DHCA determined that certain files may have been accessed and / or acquired without authorization. DHCA then undertook a comprehensive review of those files and, on or about January 12, 2026, learned that some of your personal information was contained within the potentially affected data which is the reason for this notification. Please note that DHCA has no evidence of the misuse, or attempted misuse, or any potentially impacted information.

What Information Was Involved. The information may have included your name together with <<Variable Data 1: Exposed Data Elements>>. Please note that your medical ID was not included in the data set involved with this Incident.

What We Are Doing. As soon as DHCA discovered this incident, DHCA took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. DHCA is also offering you complimentary identity protection services through IDX, a leader in consumer identity protection. These services include 24 months of credit monitoring,[1] dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is April 16, 2026.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you through IDX by calling 1-844-267-5085, going to https://app.idx.us/account-creation/protect, or scanning the QR image and using the enrollment code provided above.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 1-844-267-5085 Monday through Friday from 9 am – 9 pm Eastern Time.

[1] To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

We take your trust in us and this matter very seriously. We sincerely apologize for any inconvenience this may have caused and want to assure you that protection of your personal information remains our top priority.

Sincerely,

Daniel H. Cook Associates, Inc.
1040 6th Avenue
New York, NY 10018

Steps You Can Take to Help Protect Your Personal 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 (the "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 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 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
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
https://oag.maryland.gov
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.