



Maria Efaplatmidis
Partner
175 Pearl Street Suite C-402
Brooklyn, NY 11201
718.719.6475
mefaplatmidis@constangy.com

December 10, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Security Incident

To Whom it May Concern:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Costello, Cooney & Fearon, PLLC (“CCF”), a law firm based in New York, in connection with the data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On May 8, 2024, CCF became aware of unusual activity related to its network. In response, CCF took immediate steps to secure its digital environment and promptly launched an investigation. The investigation conducted by the third-party cybersecurity experts determined that an unknown actor accessed and acquired certain data without authorization on March 26, 2024.

On December 4, 2024 CCF confirmed that certain personal information may have been impacted and then took steps to effectuate notification to potentially impacted individuals as quickly as possible. Please note that there is currently no evidence of fraud or misuse of any of the data, only evidence that data was accessed or acquired without authorization.

2. Number of Affected Maryland Residents & Information Involved

The incident involved personal information for ten (10) Maryland residents. The information involved in the incident for the affected residents may have included name, Social Security number and driver’s license or state identification number.

3. Notification to the Affected Individuals

On December 10, 2024, a notification letter was sent to the affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps these individuals can take to help protect their information. The notification letter also offers the individuals the opportunity to enroll in 12 months of complimentary identity protection services through IDX, including credit monitoring, and identity remediation services, as well as access to a call center, should the individual have questions about the incident. A sample notification letter sent to the impacted individuals is included with this correspondence.

4. Steps Taken Relating to the Incident

In response to the incident, CCF retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. CCF also implemented additional security measures to further harden its email environment in an effort to prevent a similar event from occurring in the future. CCF also reported this incident to the Federal Bureau of Investigation.

Finally, CCF is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above. CCF has also established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns.

5. Contact Information

CCF remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Maria Efaplatidis at mefaplatidis@constangy.com.

Sincerely,

A handwritten signature in dark ink, appearing to read 'MEF', with a stylized flourish extending to the right.

Maria Efaplatidis
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Notification Letter



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

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

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

December 10, 2024

Re: Notice of Data Security Incident/Data Breach

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

Costello Cooney & Fearon PLLC (“CCF”) is writing to inform you of a data security incident that may have involved your personal information. Please read 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 Happened? On May 8, 2024, CCF experienced a network disruption. We immediately took steps to secure our network environment and engaged cybersecurity experts to conduct an investigation to determine what happened. The investigation determined that certain files may have been acquired without authorization on or about March 26, 2024. We then worked with a third-party vendor to conduct a comprehensive review of the data to determine whether personal information may have been involved. After a thorough review of the data, on December 04, 2024, it was determined that some of your personal information was present in the impacted data set.

What Information was Involved? The information potentially involved may include your name, and <<Breached Elements>>.

What We Are Doing. As soon as we discovered the incident, we took the steps described above and took steps to minimize the risk of a similar incident occurring in the future. We notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable.

Although we have no evidence that your information has been misused, we are offering the opportunity to enroll in complimentary identity protection services through IDX, an identity protection and assistance expert. These services include <<12/24>> months of credit monitoring and CyberScan (dark web) 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. You can enroll in the complementary services offered to you through IDX identity protection services by calling 1-866-750-6583 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 A.M. – 9:00 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 March 10, 2025.

For More Information: You can contact IDX at 1-866-750-6583 if you have questions about the incident or the enrollment.

We take this event and the security of information in our care seriously. We deeply regret any concern or inconvenience that this incident may cause you.

Sincerely,

Costello Cooney & Fearon PLLC

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).

Request a Copy of Your 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 <https://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 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a 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 <https://www.annualcreditreport.com>.

Put a 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 (FTC)

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/articles/pdf-0096-fair-credit-reporting-act.pdf>.