



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

May 3, 2024

VIA ONLINE SUBMISSION

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: IDTheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Dohman, Akerlund & Eddy, LLC (“DA&E”), an accounting firm based in Nebraska, 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 February 28, 2024, DA&E became aware of unusual activity related to its network. In response, DA&E 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 April 1, 2024 DA&E 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 six (6) Maryland residents. The information involved in the incident for the affected Maryland residents may have included name and Social Security number.

3. Notification to the Affected Individuals

On May 3, 2024, a notification letter was sent to the affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps this individual can take to help protect their information. The notification letter also offers the individual the opportunity to enroll in 12 months of complimentary Cy-Ex identity protection services through Epiq, 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 individual is included with this correspondence.

4. Steps Taken Relating to the Incident

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

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

5. Contact Information

DA&E 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 Efaplatmidis at mefaplatmidis@constangy.com.

Sincerely,

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

Maria Efaplatmidis
Constangy, Brooks, Smith & Prophete, LLP

May 3, 2024
Page 3

Encl.: Sample Notification Letter

Dohman, Akerlund & Eddy, LLC

Return Mail Processing
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

To Enroll, Please Call:

866.622.9303

Or Visit:

[URL](#)

Enrollment Code: <<Activation Code>>

<< First Name>> << Last Name>>

<<Address1>>, <<Address2>>

<<City>>, <<State>> <<Zip>>

<<Date>>

Re: Notice of Data Security Incident

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

Dohman, Akerlund & Eddy, LLC ("DA&E") 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 February 28, 2024, DA&E 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 compromised on or about February 28, 2024. We then conducted a review of the affected data to determine whether personal information may have been involved. After a thorough review, on April 1, 2024, it was determined that some of your personal information was present in the data set.

What Information was Involved? The information involved may include your name and Social Security number.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also implemented additional measures to reduce 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.

We are also offering you the ability to enroll in <<12/24>> months of complimentary credit monitoring and identity protection services through CyEx,

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 CyEx identity protection services, which are offered at no cost to you.

To enroll in CyEx Identity Defense visit [URL](#),

1. Enter your unique Activation Code listed at the top of this letter
Enter your Activation Code and click 'Redeem Code'.
2. Create Your Account
Enter your email address, create your password, and click 'Create Account'.
3. Register
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. Complete Activation
Click 'Continue to Dashboard' to finish enrolling.

Please note the deadline to enroll in these complimentary services is <<Enrollment Deadline>>. Please do not discard this letter, as you will need the Activation code provided above to access services.

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 888-841-5015, Monday through Friday, 9am – 9pm Eastern time. Epiq representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

DA&E values its clients and the relationships we have established in our community throughout the years. We deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Dohman, Akerlund & Eddy, LLC

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 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>.