



Richard Goldberg, Partner & Vice-Chair
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
rgoldberg@constangy.com
Mobile: 917.744.1760

March 25, 2024

VIA Website Portal

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
Tel: 207-626-8800
Email: breach.security@maine.gov

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP represents Southwest Boston Senior Services, Inc. (d/b/a Ethos), a non-profit organization which provides services such as meal delivery to people in need in the Boston area, in connection with a recent data security incident described in greater detail below.

1. Nature of the Security Incident

In November 2023, Ethos suffered a cybersecurity incident in which its network was encrypted and a monetary demand for decryption was made. There was minimal interruption of services to the community served by the non-profit entity. Ethos immediately terminated unauthorized access to the network and began an investigation to determine what happened. Ethos was able to restore full operations and obtain assurance of the destruction of any removed data. Once it appeared that some sensitive data may have been accessed during the incident, the relevant data was mined and a notification list was formed, this investigation ending on March 13, 2024. This list was used to notify potentially involved people. Employees of Ethos whose data may have been involved were also notified of the incident.

2. Number of Affected Maine Residents & Information Involved

The incident involved personal information for approximately three (3) Maine residents. The information involved in the incident was not the same for all people. The data involved for at least some of the people included name, address, Social Security number, and date of birth. Ethos has no reason to believe that the information involved has been or will be published, shared, or otherwise misused.

3. Notification to Affected Individuals

On March 22, 2024, notification letters were sent to the affected Maine residents by First Class Mail. The notification letter provides resources and steps the individual can take to help protect their information. Where a Social Security number was involved in the incident, the notification letter also offers twenty-four months of complimentary identity protection services including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed. Ethos is also issuing a press release and placing notice on its website for 90 days.

4. Measures Taken to Address the Incident

Ethos terminated the unauthorized access on its network and began an investigation into what happened. Ethos has sent notices to the potentially affected individuals and is providing them with steps they can take to protect their personal information as discussed above and reporting the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion). Ethos also has made changes to its hardware and software, conducted training, and has instituted additional security measures.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at RGoldberg@constangy.com or 917.744.1760.

Sincerely,



Richard Goldberg
Constangy, Brooks, Smith & Prophete LLP

Encl.: Sample Notification Letter



<<first>> <<last>>
<<Address1>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:




Or Visit:
<https://response.idx.us/ethos>

Subject: Notice of Data <<variable 1>>

Dear <<first>> <<last>>:

I am writing to inform you of a data security incident that may have involved your personal information. We take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened. On March 13, 2024 we determined that your information may have been involved in a cybersecurity incident. We became aware of unusual network activity on November 18, 2023. We immediately engaged cybersecurity experts to investigate and help secure our network. The investigation determined that certain data may have been acquired without authorization. While we have no information that anyone’s data has been misused, some of your information may have been involved in the incident.

What Information Was Involved. The potentially affected information may have included your name, address, and <<Information field>>.

What We Are Doing. As soon as Ethos discovered the incident we took the steps described above and implemented measures to enhance network security. We reported the incident to law enforcement and will assist in their investigation. In addition, we have secured the services of IDX to provide credit monitoring and identity theft restoration services at no cost to you for 24 months. IDX is a global leader in risk mitigation and response, and the IDX team has extensive experience helping people who have sustained an exposure of confidential data. Your services include credit monitoring, fraud consultation, and identity theft restoration.¹

Scan the QR code above or visit <https://response.idx.us/ethos> to activate and take advantage of your identity monitoring services. You have until June 22, 2024 to activate your identity monitoring services.
Membership Number: <<ENROLLMENT CODE>>

What You Can Do: This letter includes information about additional steps you can take to protect your information. You can also enroll in the identity protection services, which are offered to you at no cost, using the instructions above. Please note the deadline to enroll in these complimentary services is June 22, 2024. Please do not discard this letter, as you will need the Membership Number provided above to access services.

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

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 1-888-827-5593 Monday through Friday from 9:00 am – 9:00 pm Eastern Time.

We take your trust in us and this matter very seriously. We regret any worry or inconvenience this may cause.

Sincerely,

Ethos
555 Amory Street
Jamaica Plain, MA 02130
617-522-6700

STEPS YOU CAN TAKE TO 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 (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 <http://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 <http://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, 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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.