



Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, NY 11201
dmcmillan@constangy.com
Mobile: 718.614.8371

April 29, 2024

VIA ELECTRONIC MAIL

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

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Worthen Industries, Inc. (“Worthen”) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you, in accordance with Maryland’s statute, that this incident may have affected the personal information of two (2) Maryland residents.

1. Nature of the Security Incident

On January 13, 2024, Worthen became aware of unusual activity in its network. Upon discovering this activity, Worthen’s internal security team took immediate steps to secure our network. Worthen also engaged a team of external cybersecurity experts to assist in its response and conduct an investigation to determine what happened and whether any data within its environment may have been impacted.

The investigation revealed that an unauthorized actor gained access to Worthen’s systems between December 28, 2023 and January 14, 2024, and acquired certain data. Following a comprehensive review, Worthen determined on March 15, 2024 the data contained personal information. Since that time, Worthen has been working to gather contact information needed to provide individual notification.

2. Number of Maryland Residents Involved

On April 10, 2024, Worthen notified two (2) Maryland residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

The personal information involved in this incident varied by individual but included name, Social Security number, passport number, and health insurance information.

3. Steps Taken to Address the Incident

As soon as Worthen discovered this unusual network activity, it took steps to secure the affected system and launched an investigation to determine whether, and to what extent, personal information had been accessed or acquired without authorization. Worthen has also implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, Worthen is providing individuals with information about steps that they can take to help protect their personal information, and offering all impacted individuals the opportunity to enroll in complimentary credit monitoring and identity protection services.

4. Contact Information

Worthen remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 718-614-8371 or by e-mail at dmcmillan@constangy.com. Please let me know if you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "D. McMillan", followed by a horizontal line extending to the right.

David McMillan
Partner, Cybersecurity & Data Privacy Team

Enclosure: Sample Notification Letter



4145 SW Watson Avenue, Suite 400,
Beaverton, OR 97005

<<FirstName>> <<LastName>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<ZIP>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

April 10, 2024

Re: Notice of Data <<Security Incident/Breach>>:

Dear <<FirstName>> <<LastName>>:

We are writing to inform you of a data security incident that may have affected your personal information. At Worthen Industries, Inc. ("Worthen"), we take the privacy and security of personal information very seriously. That is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to activate your complimentary credit monitoring and identity protection services.

What Happened. On January 13, 2024, Worthen became aware of unusual activity in our network. Upon discovering this activity, our internal security team took immediate steps to secure our network. We also engaged a team of external cybersecurity experts to assist in our response and conduct an investigation to determine what happened and whether any data within our environment may have been impacted.

The investigation revealed that an unauthorized actor gained access to our systems between December 28, 2023 and January 14, 2024, and acquired certain data. Following a comprehensive review, Worthen determined on March 15, 2024 that some of your information was included among the potentially impacted data. We then worked to gather contact information necessary to provide you with this notice as quickly as possible.

What Information Was Involved. The potentially affected information may have included your <<Data Elements>>.

What We Are Doing. As soon as Worthen discovered the incident, we took the steps described above. Worthen also reported the matter to the FBI and will cooperate with any resulting investigation. Further, Worthen implemented additional measures to enhance our network security and minimize the risk of a similar incident occurring in the future.

Additionally, to help relieve concerns and to help protect your identity following this incident, Worthen is offering you <<12 / 24>> months of complimentary credit monitoring and identity monitoring services through IDX, A ZeroFox Company, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include credit and identity protection services, 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: We recommend that you activate your complimentary IDX services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the enrollment code provided above. Representatives are available from 9:00 a.m. to 9:00 p.m. Eastern Time from Monday to Friday. Please note the deadline to enroll is July 10, 2024. In addition, we recommend that you review the guidance included with this letter about additional steps you can take to protect your personal information.

For More Information. Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call 1-800-939-4170 Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can answer any questions or concerns you may have.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Worthen Industries, Inc.
3 East Spit Brook Road
Nashua, NH 03060-5783

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>.