



**OGLETREE, DEAKINS, NASH,
SMOAK & STEWART, P.C.**

Attorneys at Law

Riverfront Plaza - West Tower
901 East Byrd Street, Suite 1300
Richmond, VA 23219
Telephone: 804-663-2330
Facsimile: 804-225-8641
www.ogletree.com

Scott A. Siegner
804-663-2342
scott.siegner@ogletree.com

March 10, 2022

By Email to: Idtheft@oag.state.md.us

Brian E. Frosh, Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: *Security Breach Notification*

Dear Mr. Frosh:

This firm represents, iBASIS, Inc. (“iBASIS”), headquartered in Lexington, Massachusetts. Pursuant to The Personal Information Protection Act, Md. Code Comm. Law §14-3504, iBASIS provides the following security breach notification:

I. Nature of the Security Breach & Information Compromised

On January 30, 2022, iBASIS identified that it had been targeted as part of a ransomware attack. iBASIS immediately took steps to secure its systems, conducted a thorough forensic investigation using an independent cybersecurity team, and notified law enforcement. Through its investigation, iBASIS determined that an unauthorized party gained access to some of its servers on January 29, 2022.

The affected servers contained the names, social security numbers, and, in some cases, passport numbers of current and former employees of iBASIS. Upon receiving notice of the ransomware attack, iBASIS immediately implemented various measures to eliminate unauthorized access to the affected servers and bolster the security of its network. **At this time, iBASIS does not have any evidence that the personal information listed above that was on the affected servers has been made public or that any identity fraud has occurred in relation to the individuals involved.**

II. Number of Maryland Residents Involved

Total MD Residents Involved: 1

III. Steps Taken by iBASIS to Restore the Integrity of Its Network

iBASIS has taken the following steps to restore the integrity of its network in response to the ransomware attack:

- Installed end point protection on all servers and laptops;
- Blocked traffic from suspected IP addresses;
- Blocked outbound traffic from iBASIS servers by default;
- Rebuilt and redeployed the impacted server with updated security measures; and
- Implemented enhanced security policies and guidelines to further protect the iBASIS network.

IV. Notification to Maryland Resident

iBASIS will mail a notification letter to the affected Maryland resident on March 11, 2022, in accordance with Md. Code Comm. Law §14-3504.¹ As noted in the letter, iBASIS will also offer the resident two years of complimentary credit and identity monitoring services through Identity Force. A copy of the notification letter is enclosed as **Exhibit A**.

* * * * *

Feel free to contact me at 804-663-2342 or scott.siegner@ogletree.com if you have any questions or would like to discuss further.

Sincerely,



Scott A. Siegner

SAS:cln

¹ This notification is not, and does not constitute, a waiver of iBASIS's objection that Maryland lacks personal jurisdiction over iBASIS regarding any claims related to this date security breach.

March 10, 2022

[NAME OF INDIVIDUAL]

[ADDRESS OF INDIVIDUAL]

Subject: NOTICE OF DATA BREACH

Dear [NAME OF INDIVIDUAL]:

At iBASIS protecting personal information of our employees is a priority. In this regard, we regret to inform you that iBASIS, Inc. has become aware that a breach of your name and social security number may have occurred. We are profoundly sorry that this occurred. In addition to steps we are taking to prevent any future breaches, we have included information in this letter regarding actions you may take to further protect your own information.

What Happened

It appears that unauthorized person(s) accessed iBASIS's database containing personally identifiable confidential information. The breach was identified immediately after it occurred on January 29, 2022. Upon learning of the unauthorized access, iBASIS immediately notified appropriate authorities and continues to work with such authorities to address the issue.

What Information Was Involved

The breach involved a database that contains employee names, social security numbers, and, in some cases, passport numbers.

What Are We Doing

Upon discovery of the incident, the company immediately commenced an investigation and contained the incident with the assistance of an independent cybersecurity team. We confirmed that all operational systems, analytics, and communication systems were secure and unaffected. The impact was limited and contained by the swift action of our security and systems teams who implemented various measures designed to prevent the recurrence of similar incidents.

iBASIS
10 Maguire Road, Bldg. 3
Lexington, MA 02421

Tel
1.781.430.7500

Fax
1.781.430.7300

Email
contact@iBASIS.net

In addition, because the unauthorized hacking of the iBASIS data may have exposed your social security account, iBASIS has contracted with Identify Force, a credit monitoring service, which can monitor your credit, free of charge for up to 24 months.

Please let us know if you want to use such a service and we will provide all relevant information to enroll.

What You Can Do

As additional precautionary measures you may want to consider taking the following steps to protect yourself from potential harm resulting from the breach:

- **Contact credit reporting bureaus** - There are three major credit reporting bureaus. Their contact information is listed below. We recommend that you contact at least one of the bureaus and place a fraud alert/security freeze on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert/security freeze, the other two bureaus will be notified automatically of the fraud alert/security freeze. Placing a fraud alert/security freeze on your report is free of charge.

Equifax

P.O. Box 740256
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian

Fraud Victim Assistance
P.O. Box 9554
Allen, TX 75103
1-888-397-3742
www.experian.com

TransUnion

National Consumer Assistance

Fraud Victim Assistance Division

P. O. Box 2000

Chester, PA 19016-2000

1-800-680-7289

www.transunion.com

- Order your credit reports. By establishing a fraud alert/security freeze, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. You are entitled to receive a free credit report annually from each of the three credit bureaus. We recommend that you space out your requests so that you receive one free credit report every four months. For example, request a report from Equifax immediately, a report from Experian four months from now and a report from TransUnion four months later. Examine each report closely and look for signs of fraud such as credit accounts that are not yours.
- Continue to monitor your credit reports. Even though a fraud alert/security freeze has been placed on your account and you have credit monitoring service, you should continue to monitor your credit reports to ensure that an imposter has not opened an account with your personal information.
- Review the below additional information regarding protecting personal information

Social Security Administration: The Social Security Administration provides information about protecting your personal information: <https://blog.ssa.gov/protecting-your-social-security-number-from-identity-theft/> ; <https://www.ssa.gov/pubs/EN-05-10064.pdf>. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

Federal Trade Commission: The FTC website has further information regarding

preventing fraud and identity theft, including additional information about “fraud alerts” and “security freezes,” and about how to monitor and protect your credit and finances:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
(202) 326-2222
1-877-382-4357
www.consumer.ftc.gov/features/feature-0014-identity-theft
www.IdentityTheft.gov

Maryland Attorney General’s Office: The Maryland Attorney General’s Office may have additional information regarding protecting your personal information:

Maryland Attorney General’s Office
200 St. Paul Place
Baltimore, MD 21202,
1-888-743-0023
1-410-576-6300
www.oag.state.md.us

Again, we very much regret this situation occurred and apologize for any concern this may cause you personally.

For further assistance, additional information, or questions, please feel free to contact us.

Sincerely,

Paul Heilbronner
EVP, Human Resources