McDermott
Will & Emery

Boston Brussels Chicago Dallas Düsseldorf Frankfurt Houston London Los Angeles Miami
Milan Munich New York Orange County Paris Rome Seoul Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

David Quinn Gacioch
Attorney at Law
dgacioch@mwe.com
+1 617 535 4478

VIA EMAIL / attorneygeneral@doj.nh.gov

April 20, 2016

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification for NetBrain Technologies, Inc.

To Whom It May Concern:

This firm represents NetBrain Technologies, Inc. and we write to formally inform you of a recent data security incident affecting NetBrain, following the informal notification that we provided to you by telephone on March 4th and the following week. The names, addresses, social security numbers and compensation and tax withholding information of certain current and former NetBrain employees were obtained by an unauthorized third party in the incident.

On March 3, 2016, an unauthorized person or person(s) posing as a senior NetBrain executive emailed a more junior NetBrain employee requesting copies of all 2015 W-2 forms. The employee replied to the email, attaching the requested documents. Very shortly after the reply email was sent, NetBrain learned that the email was a scam and that the electronic W-2 forms were fraudulently obtained by an unauthorized party. NetBrain attempted to recall the email and when the recall attempts were unsuccessful, NetBrain immediately began its security incident response effort.

Within hours of the incident, NetBrain contacted the U.S. Federal Bureau of Investigation and the Internal Revenue Service to alert them of the email scam, and NetBrain representatives met with the Burlington, MA police department the following day to obtain a police report. In addition, NetBrain notified its affected current and former employees by email and/or FedEx on the day of the incident, and provided them information about filing Identity Theft Affidavits with the IRS, taking similar steps with their state taxing authorities, placing a credit/security freeze or fraud alert on credit reports and payment card accounts, and taking additional steps to protect themselves from identity theft. As another part of its review of and response to the incident, NetBrain is enhancing its data privacy and security safeguards to help ensure that a similar incident does not happen in the future.

Based on NetBrain's investigation, 18 New Hampshire residents were impacted. NetBrain intends to follow up on its immediate, informal notification to the individuals using the template letter attached—which NetBrain expects to send on or about April 20, 2016. In addition, NetBrain has offered these individuals identify theft prevention services for two years through ID Shield at no cost.

If you have any questions, please contact me at (617) 535-4478 or via email at DGacioch@mwe.com.

Sincerely,

David Quinn Gacioch

April 19, 2016

[Address]

Dear [ ]:

As you know, NetBrain Technologies, Inc. was recently the victim of a data security incident. You are receiving this letter because your personal information was among the data that was fraudulently obtained by an unauthorized third party.

On March 3, 2016, an unauthorized person or person(s) posing as a senior NetBrain executive emailed a more junior NetBrain employee requesting copies of all 2015 W-2 forms. The employee replied to the email, attaching the requested documents. Very shortly after the reply email was sent, NetBrain learned that the email was a scam and that the electronic W-2 forms were fraudulently obtained by an unauthorized party. NetBrain attempted to recall the email and when the recall attempts were unsuccessful, NetBrain immediately began its security incident response effort.

Your 2015 W-2 form that was involved this incident contained your name, address, Social Security number, and compensation and tax withholding information.

When we learned of this security incident, we immediately took steps in response. In addition to this notification, we have reported the incident to the U.S. Federal Bureau of Investigation and the Internal Revenue Service, met with the Burlington, Massachusetts police department to obtain a police report, and have notified appropriate state regulatory authorities. NetBrain is enhancing its data privacy and security safeguards to help ensure that a similar incident does not happen in the future.

In addition to the suggested actions that you may read in Attachment A (which is similar to the information we provided to you immediately after the incident), we encourage you to activate your free individual subscription to ID Shield's identify theft protection services. NetBrain has arranged for two years of identity theft protection services at NetBrain's expense. You should have received an email from ID Shield (memberservices@legalshieldcorp.com) with an account activation link. Please contact us if you have not.

We once again apologize for the inconvenience and any disruption this has caused you. If you have any questions, please do not hesitate to reach out to me at 1.781.418.9890 or to Brian Logue, Vice President, Human Resources at 1.781.418.0866.

Sincerely,

Michael Passanisi
General Counsel

cc: Brian Logue, Vice President, Human Resources

Attachment A:
Additional Information about Identify Theft Prevention

In addition to offering you the fraud remediation services described in our cover letter at our expense, we encourage you to consider the following proactive steps designed to detect and prevent financial fraud, identity theft or other misuse of your personal information:

Review your Credit Reports and Account Statements

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months online at www.annualcreditreport.com, calling toll-free at 877-322-8228, or by completing an Annual Credit Report Request Form (found at www.ftc.gov/bcp/menus/consumer/credit/rights.shtm) and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You can also purchase a copy of your credit report by contacting one of the three national credit reporting companies:

Equifax	**Experian**	**TransUnion**
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790

When you receive your credit reports, review them carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to proper law enforcement authorities, including local law enforcement. You may contact the national credit reporting agencies listed above to learn about preventing identity theft and to obtain additional information about avoiding identity theft. All U.S. residents may also contact the Federal Trade Commission ("FTC") for additional information at the following address:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Fraud Alerts

You should also consider placing a fraud alert to put your creditors and potential creditors on notice that you may be a victim of fraud. There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit or "Security" Freezes

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you put on a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift, and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*

The instructions for how to establish a credit freeze differ from state to state. You may contact the three major credit reporting companies listed above (TransUnion, Experian, and Equifax) to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Consider Applying for an Identity Protection PIN with the IRS

An IP PIN is a six-digit number assigned to eligible taxpayers that helps prevent the misuse of your SSN on fraudulent federal income tax returns. If you know your SSN has been compromised, or are concerned that it may have been, obtaining an IP PIN from the IRS can help prevent someone from using your SSN to submit a fraudulent tax return without you knowing in order to steal a refund check.

Important: You are currently unable to opt out once you get an IP PIN. You must use an IP PIN to confirm your identity on all federal tax returns you file this year and in subsequent tax years. If you e-file your return and your IP PIN is missing or incorrect, the IRS system will reject your return. Filing a paper return with a missing or incorrect IP PIN delays its processing. This is for your protection so the IRS can determine it's your return.

To get your IP PIN, you must verify your identity online at http://www.irs.gov/Individuals/Get-An-Identity-Protection-PIN. You will need to have immediate access to your email account to receive a

confirmation code. You will receive your IP PIN online once the IRS verifies your identity. The IRS will then send you a new IP PIN each December by postal mail. If you move, you must submit a change of address form to the IRS.

Visit the IRS's online page of FAQs for more information and to determine whether the IP PIN might be right for you at: http://www.irs.gov/Individuals/Frequently-Asked-Questions-about-the-Identity-Protection-Personal-Identification-Number-(IP-PIN)

What if You Find Evidence of Identity Theft or Other Suspicious Activity?

We recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission. You may contact the FTC or your state regulatory authorities to obtain additional information about avoiding identity theft.