SheppardMullin

Sheppard, Mullin, Richter & Hampton LLP
379 Lytton Avenue
Palo Alto, California 94301-1479
650.815.2600 main
650.815.2601 fax
www.sheppardmullin.com

trodewald@sheppardmullin.com

February 12, 2017

VIA ELECTRONIC MAIL

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Security Breach Notification

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. § 359-C:20, we are writing on behalf of our client NEO Tech, 9340 Owensmouth Avenue, Chatsworth, CA 91311 and its subsidiaries OnCore LLC, OnCore Manufacturing LLC and Epic Technologies to notify you of an unauthorized access to personal information of four New Hampshire residents.

On January 27, 2017, NEO Tech was the victim of an email "phishing" incident that resulted in the release of employee W-2 wage and tax data to an unauthorized recipient outside the company. An unknown person "spoofed" the email address information of NEO Tech's CEO and sent a request for employee W-2 information to an employee within NEO Tech's human resources department. The NEO Tech employee responded to the request believing it was a legitimate request originating from the CEO. The response attached an encrypted and password protected PDF file containing an electronic copy of 2016 NEO Tech employee W-2 information (which includes each affected employee's name, address, 2016 income information and Social Security Number or Individual Taxpayer Identification Number). The password for the PDF file was not specifically provided, but when a request came back asking for the password, a strong hint was provided. The same day, NEO Tech discovered the scam, and began taking steps to address it.

Four New Hampshire residents were affected by this breach. NEO Tech provided these individuals with notice of the breach on January 31, 2017, and provided the attached amended notice on February 10, 2017. NEO Tech is providing affected employees with identity monitoring and identity theft protection services for a year at no cost to employees. The services covered include monitoring services, fraud resolution services, and identity theft insurance in the event that an employee's information is misused. NEO Tech's notifications also provided affected employees with further information about steps the employees can take to protect themselves including information about placing fraud alerts, security freezes and monitoring their credit reports.

In addition, NEO Tech immediately notified the IRS Criminal Investigation and ID Theft Unit and state tax departments related to affected employees. The IRS has informed us that they will be validating the affected employees' tax returns to help prevent tax fraud. NEO Tech will continue to work with these authorities and provide the cooperation they need to investigate this incident and help protect employees from tax fraud.

NEO Tech does not have any information that employee personal information has been misused. NEO Tech is conducting a thorough internal investigation. This investigation is not yet complete, but NEO Tech is committed to taking additional steps it can identify to prevent similar incidents from occurring in the future.

If you have any questions or need further information, please contact me at the above contact information, or Craig Cardon, (310) 228-3700, CCardon@sheppardmullin.com.

Very truly yours,

Tenaya Rodewald
for SHEPPARD, MULLIN, RICHTER & HAMPTON LLP

NEOTech
NATEL EPIC OnCore

9340 Owensmouth Avenue
Chatsworth, CA 91311
818-734-6500
Fax 818-734-6520
neotech.com

AMENDED NOTICE OF DATA BREACH

February 10, 2017

Dear XXX:

We are writing because of a recent, isolated cyber incident that resulted in the disclosure of certain NEO Tech employee personal information on January 27, 2017. NEO Tech and its management team are taking an aggressive approach to this incident in order to help employees protect against potential fraud.

What happened

On Friday, January 27, 2017, NEO Tech was the victim of an email "phishing" incident that resulted in the release of employee W-2 wage and tax data to an unauthorized email recipient outside the company. This was an isolated incident that did not involve an intrusion into our computer systems or network.

What information was involved

The following NEO Tech employee information: a copy of your 2016 Form W-2, which includes your name, address, 2016 income information and Social Security Number.

What we are doing

We have contacted the IRS Criminal Investigators and ID Theft Unit, and the affected State Franchise Tax Board (FTB) theft units and have provided the information that was released. We will continue to work with them and provide the cooperation they need to investigate this incident and help protect you from tax fraud. If you are due a refund, the FTB and the IRS have informed us that they will be validating your return and there may be a delay in receiving your refund as a result of this process.

NEO Tech will be providing you with identity monitoring and identity theft protection services for a year at no cost to you from Experian.

Experian will provide Fraud Resolution assistance and if activated with Experian, fraud detection tools available through ProtectMyID® Elite as a complimentary one year membership from the date of activation.

Experian Fraud Resolution assistance is immediately available to you. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-441-6943 and provide engagement **# [code]** as proof of eligibility. If, after discussing your situation with an agent, it is determined that fraud resolution support is needed then an Experian Fraud Resolution agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition.) Please note that this offer is available to you until February 10, 2018 and does not require any action on your part at this time. The Terms and Conditions for the Fraud Resolution assistance are located at www.experian.com/fraudresolution. You will also find self-help tips and information about identity protection at this site.

For additional fraud detection services you will need to enroll in Experian's ProtectMyID® Elite plan. You will not need a credit card to enroll as membership for one year is covered. You will have access to the following services once you enroll:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*[1]:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

To enroll in the ProtectMyID® Elite Plan:

- **Enroll by**: **February 10, 2018** (Your code will not work after this date.)
- **Enroll on** the ProtectMyID website: **www.protectmyid.com/enroll**
- Provide your **activation code**: **[code]**

If you have questions about the incident, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please

[1] *Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

contact Experian's customer care team at 877-441-6943 by February 10, 2018. Be prepared to provide engagement number **# [code]** as proof of eligibility for the fraud resolution services by Experian.

What You Can Do

Additional steps you can take to protect yourself from potential identity theft and tax fraud

1. To minimize the risk of tax fraud, we recommend that you file your tax return as soon as possible.

2. You may also complete Form 14039-Identity Theft Affidavit (https://www.irs.gov/pub/irs-pdf/f14039.pdf) and submit this form to the Internal Revenue Service ("IRS") by fax or mail. While the IRS Criminal Investigators and ID Theft Unit has informed us, that it is not necessary to file this form at this time, it is recommended that you file this form if you:

- Receive an efile reject when you attempt to file your return via efile.
- Receive IRS correspondence requesting validation of the filing of their tax return and they have not yet filed, or
- You have filed and the IRS sends a notice that you have already filed a return, or the IRS needs more information related to their 2016 tax return.

3. If you will not be filing your tax return in the near future, you may also call the IRS at 800-908-4490 to check the status of your account and make sure there has not been any suspicious activity.

4. For more information from the IRS, please see the publication on Identity Protection: Prevention, Detection and Victim Assistance at https://www.irs.gov/Individuals/Identity-Protection.

5. Place a 90-day Fraud Alert. Because your Social Security number was involved, we recommend that you place a fraud alert on your credit file. An initial fraud alert lasts 90 days and tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit reporting companies. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three bureaus will send you your credit report to review, free of charge.

To place a fraud alert on your credit report, contact one of the credit reporting companies (you do not need to contact all of them):

TransUnion	**Equifax**	**Experian**
www.transunion.com	www.equifax.com	www.experian.com
Phone: 800-680-7289	Phone: 888-766-0008	Phone: 888-397-3742
P.O. Box 2000	P.O. Box 740241	P.O. Box 4500
Chester, PA 19016	Atlanta, GA 30374	Allen, TX 75013

6. Consider Placing a Credit (Security) Freeze. Also known as a security freeze, this tool prevents others from seeing your credit report and credit score unless you decide to lift the freeze. There is a small fee for placing a freeze, and you must contact each of the credit reporting companies separately. In addition, please note that when a freeze is in place you will have to take additional steps before you can apply for credit or permit others—such as prospective landlords—to view your credit report. You will need to lift the freeze temporarily, either for a specific time or for a specific party. For California residents, the credit reporting companies must lift the freeze within 3 business days, and the fee for lifting the freeze temporarily is $10 for a date-range lift, or for a lift for a specific creditor. You can find further information about credit freezes at the following website from the California Office of the Attorney General: https://oag.ca.gov/idtheft/facts/freeze-your-credit.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Trans Union Security Freeze Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com
Phone: 888-909-8872

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
Phone: 800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com
Phone: 888-397-3742

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

7. Review Your Credit Report and Check Your Account Statements Periodically. The Federal Trade Commission (FTC) recommends that you remain vigilant by reviewing your account statements and checking your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.

8. If You Find Suspicious Activity. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, contact local law enforcement and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

For More Information

Additional information about identity theft and fraud is available through the FTC at:

Website:	https://www.consumer.ftc.gov/
Mailing address:	Bureau of Consumer Protection, Federal Trade Commission 600 Pennsylvania Ave., NW Washington, DC 20580
Phone:	877-438-4338

Additional information is also available at the web site of the California Office of Privacy Enforcement and Protection at www.privacy.ca.gov.

As noted, we will continue to work with the IRS Criminal Investigators and ID Theft Unit and other law enforcement agencies. This notice has not been delayed as a result of any such efforts.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact your local HR representative or Zareen Mohta at xxxxx@neotech.com.

Regards,

Laura L. Siegal
CFO