CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

ERNEST KOSCHINEG
ekoschineg@c-wlaw.com

JORDAN MORGAN
jmorgan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

August 10, 2021

Via First Class Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Breach Notification

To Whom It May Concern:

I serve as counsel for NE Peptide, LLC. ("NE Peptide"), and provide this notification to you of a recent data security incident suffered by NE Peptide. On or about January 7, 2021, NE Peptide became aware of a potential compromise to an email account belonging to an employee. Upon discovery, NE Peptide performed a password reset for the affected account and swiftly engaged a third-party team of forensic experts to perform a full forensic investigation to determine the incident's scope. Following a full and thorough investigation, it was confirmed that only one (1) employee email account was subject to unauthorized access during this incident. Upon confirmation of the unauthorized access to the employee email account, NE Peptide immediately investigated whether the affected email account contained individuals' sensitive information. On July 12, 2021, following a thorough investigation, NE Peptide determined that the unauthorized access may have allowed access to limited individual's personal information.

At this time, NE Peptide is aware of thirteen (13) New Hampshire residents who may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional New Hampshire residents are potentially affected.

NE Peptide will promptly notify all affected individuals on August 11, 2021, and offer all affected New Hampshire residents complimentary credit monitoring for twelve (12) months. A copy of the draft notification letter is attached, which outlines the incident and provides affected individuals with additional resources to protect their identity and monitor the credit history and personal accounts. As the letter indicates, NE Peptide will be offering credit monitoring and identity restoration services at NE Peptide 's expense. NE Peptide is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: Jordan L. Morgan
Jordan Morgan, Esq.

NE Peptide LLC

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

August 11, 2021

RE: Important Security Notification. Please read this entire letter.

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident experienced by NE Peptide, LLC. ("NE Peptide") that may have involved your personal information described below.

NE Peptide takes the privacy and security of all information very seriously. We have no evidence that any of the impacted information was viewed or misused during this incident, but we want to be as transparent as possible to ensure the safety of your personal information. With this in mind, I am writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to let you know about complimentary credit monitoring services that we are offering you.

What Happened:

On or around January 7, 2021, NE Peptide became aware of a potential compromise to an email account belonging to an employee. Upon discovery, NE Peptide performed a password reset for the affected account and swiftly engaged a third-party team of forensic experts to perform a full forensic investigation to determine the incident's scope. Following a full and thorough investigation, it was confirmed that only one (1) employee email account was subject to unauthorized access during this incident. Upon confirmation of the unauthorized access to the employee email account, NE Peptide immediately investigated whether the affected email account contained individuals' sensitive information. On July 12, 2021, following a thorough investigation, NE Peptide determined that the unauthorized access may have allowed access to limited individual's personal information.

There is no indication that any information was actually viewed or exfiltrated from the email account; however, the forensic investigation could not rule out the possibility that an unknown third-party actor had access to an email inbox that stored this information. Therefore, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information has been viewed or misused. The personal information that could have been accessed by the unauthorized individual(s) may have included your first and last name, in combination with your <<Data Elements>>.

What We Are Doing:

NE Peptide has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Unfortunately, network intrusions have become more common and this incident

experienced by NE Peptide is similar to other experiences by other companies across the country. Upon learning of this incident, we immediately secured the affected account, reset passwords, and took steps to enhance the security of all information to help prevent similar incidents from occurring in the future. We retained a third-party forensic firm to conduct a thorough investigation and are offering you complimentary credit monitoring and identity protection services.

Credit Monitoring:

As a safeguard, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring service is enclosed.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is November 11, 2021.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password and take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

New England Peptide takes information security very seriously. While it is regrettable this potential exposure occurred, please be assured we are taking all appropriate actions to rectify the situation and prevent such incidents in the future.

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1-800-939-4170, Monday through Friday, 9 AM to 9 PM ET, or write us at 65 Zub Lane, Gardner, MA 01440.

Sincerely,

David Gavlik

Chief Financial Officer
NE Peptide LLC.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

We are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is November 11, 2021. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069

TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection. may be contacted at 140 East 60th Street, New York, NY 10022.