MULLEN COUGHLIN LLC

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 27, 2017

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

We represent Pacific Quest, 15 Kanoa Street, Hilo, Hawaii 96720, and are writing to notify your office of an incident that may affect the security of personal information relating to 3 New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Pacific Quest does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On April 10, 2017, Pacific Quest learned that it was the victim of an email spoofing attack that occurred on January 30, 2017 by an individual pretending to be its Executive Director. A request was made from what appeared to be a legitimate Pacific Quest email address for all 2016 Pacific Quest employee IRS Form W-2 information. Unfortunately, copies of all 2016 employee W¬2 forms were provided before Pacific Quest discovered that the request was fraudulent. Since discovering is incident, Pacific Quest has been working tirelessly to investigate and to mitigate the impact of the attack

Notice to New Hampshire Residents

On April 12, 2017, Pacific Quest provided preliminary notice to current employees and former employees for whom they had email addresses via email. A copy of this notice is attached here as ***Exhibit A***. On April 27, 2017, Pacific Quest will begin providing written notice of this incident to all affected current and former employees, which includes 3 New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the fraudulent nature of the email, Pacific Quest moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

Pacific Quest is providing all potentially affected individuals access to three (3) free years of credit and identity monitoring services, including identity restoration services, through AllClear ID, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Pacific Quest is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Pacific Quest also provided written notice of this incident to other state regulators as necessary. Pacific Quest has provided notice of this incident to the IRS and the FBI.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4775.

Very truly yours,

Chris DiIenno of
MULLEN COUGHLIN LLC

CJD:ab

Exhibit A

NOTICE OF DATA BREACH

4/12/2017

Dear PQ Employee:

We are contacting you because we have learned of a serious data security incident that involves personally identifiable information.

We have become aware of our victimization through a criminal email phishing scam that has compromised full names, social security numbers and wage information. Once the security breach was discovered the company took action to report the crime to local authorities, the IRS and the FBI.

We regret to inform you that you are among the people whose personal information was compromised. Although we do not have specific evidence or information regarding if your individual information was used for malicious purposes, we are notifying those whose data was exposed to help them address security and other concerns.

We advise you to remain vigilant by reviewing account statements and monitoring free credit reports. Per the IRS this information may most commonly be used for tax identity theft or to open fraudulent accounts.

There are some actions you may take to protect yourself at this point. We strongly advise that you take these steps immediately.

First is to request a free credit report and review the report for suspicious activity. To order your free credit report, visit www.annualcreditreport.com or call: 877-322-8228.

If you are concerned that there might be fraudulent activity, you should contact credit-reporting agencies to initiate a fraud-alert process. Any one of the three major agencies listed below should be contacted. The initial alerted agency will notify the other two. Each of the agencies will mail credit reports to you at no cost.

The credit agencies are:

- Equifax (800) 685-1111
- Experian (888) 397-3742
- TransUnion (800) 916-8800

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

If you feel you have been a victim of identity theft, you should also follow the "Steps for Identity Theft Victims" which include:

- Contacting one of the three credit bureaus to place a "fraud alert" on their account; they may consider placing a "credit freeze" which offers more protection.
- File a complaint with the Federal Trade Commission, the lead federal agency on identity theft issues.
- Review FTC www.identitytheft.gov information for additional steps to recover from identity theft.

It is also important for you to review the IRS guide to identity theft: https://www.irs.gov/uac/taxpayer-guide-to-identity-theft.

Additionally, we are offering all affected employees a credit monitoring service for one year from the date of initiation. We are in the process of securing this contract and setting up access information. Information will be provided to you as soon as it is available.

It may also be prudent to notify your bank in the event that anyone tries to access your accounts fraudulently.

Pacific Quest is committed to making our data as secure as possible. As a company we regularly review computers, mobile devices and systems for break-ins, viruses, or other problems. In response to this incident we are conducting a full review of our cyber security policies. We will continue to be vigilant with our efforts to protect our information.

The IRS is reporting an increase of this type of crime across the nation and that it is spreading from companies to school districts and other organizations. We apologize for any distress this situation causes you. We are ready to assist you and will be in touch with updates as they are available.

Should you require any further information and assistance, please contact Brittny in Human Resources, brittny.deacy@pacificquest.org.

Sincerely,

Pacific Quest

Exhibit B

PACIFIC QUEST
SUSTAINABLE GROWTH
Processing Center • P.O. BOX 141578 • Austin, TX 78714

STATE OF NH
DEPT OF JUSTICE
2017 MAY -2 AM 10: 25

00005
00002 ACD1234
John Q. Sample
1234 MAIN STREET
ANYTOWN US 12345-6789

April 27, 2017

Re: Notice of Data Breach

Dear John Sample,

We are writing to supplement our April 12, 2017 notice regarding the recent email spoofing attack that may affect the security of your personal information. As stated in the previous notice, the email spoofing attack led to the compromise of names, Social Security numbers and wage/withholding information. Once the incident was discovered, the company took action to report the crime to local authorities, the IRS, the FBI and state revenue departments. We are providing this supplemental notice so that you have access to the resources and information to provide steps you may take to guard against identity theft or fraud.

What Happened? On April 10, 2017, we learned that Pacific Quest was the victim of an email spoofing attack that occurred on January 30, 2017 by an individual pretending to be our Executive Director. A request was made from what appeared to be a legitimate Pacific Quest email address for all 2016 Pacific Quest employee IRS Form W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before we discovered that the request was fraudulent. Since discovering this incident, we have been working tirelessly to investigate and to mitigate the impact of the attack.

What Information Was Involved? A file, including a copy of your IRS Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. All company security, storage and training systems are under a full review. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems.

As an added precaution, we have arranged to have AllClear ID protect your identity for 36 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months.

01-02-2-00

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-216-2977 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-216-2977 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-216-2977 (toll free), Monday through Saturday, 3:00 a.m. to 3:00 p.m. HST.

We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

Pacific Quest

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-800-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. One Rhode Island resident may be impacted by this incident. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.