26013

Seatrec, Inc.
1340 Specialty Dr., Suite I
Vista, CA 92081

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

Enrollment Code: [XXXXXXXX]

[First and Last Name]
[Address 1]
[Address 2]
[City, State, Zip]

February 18, 2022

Notice of Data Breach

Dear [Name],

We value you as a member of the Seatrec team and respect the privacy of your information, which is why, as a precautionary measure, we are writing to notify you that an unauthorized access of your personal information may have occurred before January 20, 2022. Although we are unaware of any actual download or misuse of your information, we are providing you this notice to ensure that you are and remain fully informed. Since learning Seatrec was the target of a phishing attack we have taken steps to prevent others from being similarly victimized, contacted service providers to help us understand the potential scope of the incident, and engaged an IT consultant to conduct a forensic investigation.

What Happened

On January 20th, 2022, we discovered that an unauthorized third party used credentials compromised in a phishing scam to access our internal network.

Upon discovering this incident, we took immediate action to lock down the impacted accounts and eject the perpetrator from the Seatrec network. Every employee has changed their passwords. Seatrec has initiated the use of Multi-Factor Authentication (MFA) for every Seatrec email account to add an extra layer of protection. With MFA enabled, when a user signs in to a MS Outlook email account, they will be prompted for their user name and password (the first factor—what they know), as well as for an authentication code from their MFA device such as a cell phone (the second factor—what they have).

At this time, there is no indication that there was any acquisition of any sensitive personal information. Nevertheless, we are providing this notice to you out of an abundance of caution because your information was available through some of the affected systems, and potential access to or acquisition of that information could not be definitively ruled out.

What Information Was Involved

Information that may have been involved includes names, contact information, government issued identification, such as driver's license or passport, tax forms, such as Form W4 or Form I9, Social Security numbers, tax identification numbers, dates of birth, birth certificates, bank account numbers, bank routing numbers, dates of employment, salary information, and other related information maintained for human resources purposes.

What Are We Are Doing

After detecting unusual activity, we took immediate steps to identify and contain the threat posed by the third party and promptly reported the incident to federal law enforcement. We are also evaluating additional measures to further enhance our protocols for the protection of your personal information. We have included in this letter steps you can take to protect your personal information.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 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.

What You Can Do

You should review the enclosed *Additional Steps You Can Take to Further Protect Your Information*. You can also take advantage of the complimentary identity theft prevention and mitigation credit monitoring services. Seatrec will pay this service for the initial twenty-four months at no cost to you.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 20, 2022.

You should remain vigilant against incidents of identity theft and fraud, review your account statements regularly, and freeze or monitor your credit reports for suspicious activity. You should also report any suspicious activity to Seatrec. Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

More Information

You will find detailed instructions for enrollment on the enclosed *Additional Steps You Can Take to Further Protect Your Information* document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

For further information and assistance, please contact me by phone (626-354-2612) or email (yi.chao@seatrec.com).

SEATREC

Very truly yours,

Yi Chao
CEO

Additional Steps You Can Take to Further Protect Your Information

Website and Enrollment. Go to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

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

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts and Credit or Security Freezes:

***Fraud Alerts*:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

***Credit or Security Freezes*:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the

freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

How do I place a freeze on my credit reports? You must separately place a security freeze on your credit file with each credit reporting agency. For information and instructions on how to place a security freeze, contact each of the credit reporting agencies identified above. Please be aware 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses above. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information above.

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

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, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. 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. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

How do I lift a freeze from my credit reports? To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including 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. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) 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 make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide 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 between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.