February 23, 2017

«First_Name» «Last_Name»
«Street_Address»
«City», «State» «Zip»

Dear «First_Name1»:

We are writing to notify you of an incident affecting your personal information. Although we are not aware at this time of identity theft specifically linked to this incident, we wanted to inform you about this situation, the steps we are taking to protect your information, and steps you may take to help protect yourself.

What happened?

On February 20, 2017, Nomad Global Communication Solutions, Inc. ("Nomad") learned that an unidentified attacker had used an email phishing scheme to obtain access to personal information contained on 2016 W-2 forms relating to current and former Nomad employees. The types of personal data affected included information listed on W-2 forms such as names, addresses, Social Security numbers, and wage information.

What is Nomad doing to protect you?

We recognize this issue can be frustrating and we are taking steps to help protect you and to safeguard personal information going forward. As an added precaution, we have arranged to have AllClear ID protect your identity for 12 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 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 877-676-0379 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**. This will not happen automatically without your personal action. You may sign up online at enroll.allclearid.com using the following redemption code: «redemption_code». Note: this code is unique to you alone.

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

Regardless of whether you choose to take advantage of the identity protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit reports, bank account activity, and financial statements for any unauthorized transactions. More information about preventing identity theft is included with this letter.

To help prevent a similar incident from happening in the future, we are evaluating our controls and will be implementing additional technical and administrative measures to enhance our information security safeguards moving forward. Employees should contact the Fraud Team (Joyce Bellwood, Clay Binford, and Joe Sullivan) immediately regarding any potentially fraudulent emails sent to their Nomad email accounts.

If you have further questions regarding this incident, you may email fraudalert@nomadgcs.com or call Joyce Bellwood at 406-755-1721 ext. 2602.

Sincerely,

Will Schmautz
President / CEO
Nomad Global Communication Solutions

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID by email at support@allclearid.com; by phone at 855-434-8077; or by mail sent to AllClear ID, Inc., 823 Congress Avenue Suite 300, Austin, TX 78701.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of the identity theft protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit www.annualcreditreport.com or call toll free at 877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 685-1111	(888) 397-3742	(800) 916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. You may contact the FTC by visiting www.ftc.gov/idtheft, calling (877) 438-4338, or writing to 600 Pennsylvania Avenue, NW, Washington, D.C., 20580.

The FTC's website includes information about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You also should contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Fraud Alerts

You also may request that the nationwide credit reporting agencies place a "fraud alert" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. Contact information for each of the three credit reporting agencies is listed above. Once one credit reporting agency processes your fraud alert, it will notify the other two, which then also must place a fraud alert in your file.

There are two types of fraud alerts. 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 and have obtained the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. If you ask for an extended alert, you will have to provide an identity theft report (generally a copy of a report you have filed with a federal, state, or local law enforcement agency), and additional information the credit reporting agency may require you to submit.

You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the toll-free numbers listed below:

Equifax	**Experian**	**TransUnion**
(888) 766-0008	(888) 397-3742	(800) 680-7289

Tax-related Identity Theft

We also recommend that you review the IRS website's resources regarding tax-related identity theft at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

For 2017, the IRS, state governments, and the tax industry joined together to enact new safeguards and take additional actions to combat tax-related identity theft. Many of these safeguards may be invisible to taxpayers, but invaluable in the fight against criminal syndicates. If you prepare your own tax return using software, you will encounter new log-on standards.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses a stolen Social Security number (SSN) to file a tax return and claim a refund that does not belong to them. You may be unaware that this has happened until you attempt to e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying that they have identified a suspicious return using your SSN and require further verification to process the return.

Know the warning signs

Be alert to the signs of tax-related identity theft. For example, you may be contacted by the IRS or your tax professional/provider indicating that:

- More than one tax return was filed using your SSN;
- You owe additional tax, refund offset or have had collection actions taken against you for a year you did not file a tax return; or
- IRS records indicate you received wages or income from an employer for whom you did not work.

Steps to take if you become a victim

In addition to the steps outline above, if your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039 (Identity Theft Affidavit) if your e-filed return is rejected because of a duplicate filing under your SSN, or if you are instructed to do so. IRS Form 14039 (Identity Theft Affidavit) is available here: https://www.irs.gov/pub/irs-pdf/f14039.pdf. You may use the fillable form that can be found on the IRS.gov website at the link above, then print and attach the completed form to your tax return and mail it to the IRS.
    - Note: you should submit a Form 14039 **only** if your Social Security number has been compromised ***and*** your e-file return was rejected as a duplicate, or if the IRS has informed you that you may be a victim of tax-related identity theft.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and your situation was not resolved, you may contact the IRS for specialized assistance at (800) 908-4490.