MEMORANDUM

TO: Team Members Employed by Wisenbaker Building Services in 2016

DATE: February 10, 2017

RE: URGENT COMMUNICATION – Preliminary Notice of Data Incident

We recently discovered that our company was the victim of an email spoofing attack today, February 10, 2017, by an individual pretending to be our owner. A request was made from what appeared to be a legitimate Wisenbaker email address for all 2016 Wisenbaker employee W-2 information. Unfortunately, copies of all 2016 employee W2 forms for our Texas employees were provided before we discovered that the request was made from a fraudulent account by someone using the name and an email address that appeared to be from our owner. We discovered the fraudulent nature of the request today and have been working tirelessly to investigate and to mitigate the impact of the attack.

Please note that this incident affects you only if you were employed by Wisenbaker in 2016 and reside in Texas. If your employment did not begin with Wisenbaker until 2017 or you reside outside of Texas, then your information has not been impacted.

The confidentiality, privacy, and security of our employee information is one of our highest priorities. While our investigation is ongoing, we felt it important to notify you about this incident, and what we are doing to investigate and respond, as quickly as possible. Here are some actions that we are taking and that we encourage you to take:

- Identity Protection. As a precaution, for those individuals affected by this incident, we are making arrangements with vendors to provide credit monitoring and restoration services at no cost to you. **The cost of this service will be paid for by Wisenbaker, and instructions for activating your protection will be included in a forthcoming letter.**
- Filing of 2016 Tax Returns. We encourage you to file your 2016 tax return as soon as possible, if you have not already done so. This is the best way to protect against a fraudulent filing with your information. You can contact the IRS at http://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 https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.
- Notice to Affected Individuals. We also will be mailing information to all impacted current and former Wisenbaker team members. This letter will include information on the credit monitoring service and enrollment instructions.
- Call Center for Employee Questions. We will establish a call center to answer common questions regarding this incident. ***However, until that call center is established, please contact Stacy Figg at*** [XXX-XXX-XXXX] ***for additional information***.
- Notice to Law Enforcement and the IRS. We will be notifying federal law enforcement of the incident. We look forward to cooperating with the FBI and state law enforcement agencies in their investigations of this incident. We also reported this

incident to the IRS so that they may take steps to monitor for attempts to file fraudulent tax returns using Wisenbaker employee information. We will also take steps, as necessary, to notify appropriate state taxing authorities of the incident.

- Information Technology Systems Review. At this time, we do not believe that our IT systems were otherwise compromised by this attack. However, our IT team is assessing the security and soundness of our systems and determining how best to prevent these types of attacks in the future.
- Employee Training. Unfortunately, even the best technology cannot prevent all cyber-attacks, particularly those intended to fool employees into providing sensitive company information. We will continue and improve upon our information security awareness and training programs for all employees.

We apologize for any inconvenience this incident causes you. Please know that we are working diligently to remedy this incident and to prevent any similar incidents from occurring in the future. If you have any questions about the contents of this notice or about the incident, please contact our Stacy Figg at [XXX-XXX-XXXX].

WISENBAKER
BUILDER SERVICES, INC.
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name1>>
<<Address>>
<<City>><<State>><<Zip>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

I am writing in follow up regarding our recent notice about the email phishing attack. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? As we mentioned in our February 10th email, we recently discovered that our company was the victim of an email phishing attack on February 10, 2017. A request was made from what appeared to be a legitimate Wisenbaker email address for all 2016 Wisenbaker Builder Services employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms for our Texas employees were provided before we discovered that the request was made from a fraudulent account. We discovered the fraudulent nature of the request on February 10, 2017 and 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 Tax 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. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Wisenbaker Builder Services has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individual who sent the fraudulent email accessed our computer network or that our IT systems were otherwise compromised by this attack. However, our IT team is assessing the security and soundness of our systems. 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. We have contacted the IRS and FBI and will be contacting the relevant state Attorneys General.

As an added precaution, we have arranged to have Experian's ProtectyMyID Elite product 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. The cost of this service will be paid for by Wisenbaker Builder Services. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. Enrollment instructions are included in the attached "Steps You Can Take To Prevent Identity Theft And Fraud."

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. 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 888-221-7299 (toll free), Monday through Friday, 8:00 a.m. to 8:00 p.m. CST, excluding U.S. holidays.

Wisenbaker Builder Services takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Joe Chiavone, Jr., CPA
Chief Financial Officer
Wisenbaker Builder Services

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.

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. 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 for one-year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.experian.com/fraudresolution. You will also find self-help tips and information about identity protection at this site.

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID® Elite as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

Ensure that you **enroll by: <<Enrollment Deadline>>**. (Your code will not work after this date.)
Visit the ProtectMyID website to enroll: **www.protectmyid.com/enroll**
Provide your **activation code: <<code>>**

If you have questions about the product, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-441-6943 by **<<Enrollment Deadline>>**. Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the fraud resolution services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is **not** required for enrollment in ProtectMyID.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

- **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.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.experian.com/fraudresolution for this information.

[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.

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 19106
800-525-6285	888-397-3742	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	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/freeze

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. 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.