TO: Team Members Employed by Baylor Evnen, LLP in 2019

DATE: April 5, 2020

RE: URGENT COMMUNICATION – Preliminary Notice of Data Incident

We discovered that our company was the victim of an email spoofing attack on Friday, April 3, 2020 by an individual pretending to be a Baylor Evnen employee. A request was made from what appeared to be a legitimate email address for 2019 Baylor Evnen employee W-2 information. Unfortunately, copies of 2019 employee W2 forms 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 legitimate. We discovered the fraudulent nature of the request on April 3, 2020, 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 Baylor Evnen in 2019. If your employment did not begin with Baylor Evnen until after 2019, 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 arranged for Kroll to protect your identity for 12 months at no cost to you. The cost of this service will be paid for by Baylor Evnen, and instructions for activating your protection are included in this email. ***We strongly encourage you to act to take advantage of these free identity protections services as soon as possible.*** 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. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

How To Activate Your Identity Monitoring Services

- You must activate your identity monitoring services by **July 10, 2020**. Your Activation Code will not work after this date.
  - Visit **https://enroll.idheadquarters.com/redeem** to activate your identity monitoring services.

Provide Your Activation Code: and Your Verification ID:

  - To sign in to your account after you have activated your identity monitoring services, please visit **https://login.idheadquarters.com/**

- Notice to Affected Individuals. We also will be mailing information to all impacted current and former Baylor Evnen team members.

- Employee Questions. If you have more questions involving this incident, please call Jarrod Crouse at (402) 475-1075.
- Notice to Law Enforcement and the IRS. We notified federal law enforcement of the incident, and we will be notifying any necessary state Attorneys General as well. We look forward to cooperating with the FBI and state law enforcement agencies in their investigations of this incident. We also are reporting this incident to the IRS so that they may take steps to monitor for attempts to file fraudulent tax returns using Baylor Evnen employee information. We will also take steps, as necessary, to notify appropriate state taxing authorities of the incident.
- Filing of 2019 Tax Returns. We encourage you to file your 2019 tax return as soon as possible, if you have not already done so. 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. If you become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you should file the IRS Form 14039, Identity Theft Affidavit, with a paper copy of the return, and mail according to the instructions. A copy of this form can be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.
- 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, with assistance from IT forensics and cyber-specialists, are 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 designed to fool employees into providing sensitive company information. We will continue to provide, and improve upon, our information security awareness and training programs for all employees.

We apologize for the 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.

Take Advantage of Your Identity Monitoring Services

We are providing you access to the following services from Kroll[1]:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who can help you determine if it is an indicator of identity theft.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Web Watcher
Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona
Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan
Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement
Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation
You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration
If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

EXHIBIT B

BAYLOR EVNEN

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We write to formally notify you, again, of an email spoofing attack that may affect the security of some of your personal information. This letter pertains to the same incident referenced in an email we sent to you a short time ago. We take this incident seriously and we are providing you with information and access to resources so that you can help protect your personal information, should you feel it is appropriate to do so.

What Happened? We discovered that our company was the victim of an email spoofing attack on Friday, April 3, 2020, by an individual pretending to be a Baylor Evnen employee. A request was made from what appeared to be a legitimate email address for 2019 Baylor Evnen employee W-2 information. Unfortunately, copies of 2019 employee W-2 forms 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 legitimate. We discovered the fraudulent nature of the request on April 3, 2020 and have continued to work tirelessly to investigate and mitigate the impact of the attack.

What Information Was Involved? 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. Baylor Evnen 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, with assistance from IT forensics and cyber specialists, are 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 contacted the IRS and FBI and will be contacting the relevant state Attorneys General.

As an added precaution, we arranged to have Kroll Inc. help safeguard your identity for 12 months at no cost to you. The cost of this service will be paid for by Baylor Evnen. It is incumbent upon you to activate these services, as we are not able to act on your behalf to activate your identity monitoring service. The identity monitoring activation instructions and unique code is contained within the preliminary email notice we sent to you a short time ago.

What You Can Do. You can review the enclosed "Steps You Can Take to Help Protect Your Information." You can also activate to receive the free identity monitoring services described above.

In addition, if you have not already done so, we encourage you to file your 2019 tax return as soon as possible. If you become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you should file the IRS Form 14039 Identity Theft Affidavit along with a paper copy of your return and mail according to the instructions on that form. A copy of this form can be found at: https://www.irs.gov/pub/irs-pdf/f14039.pdf, or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

Baylor Evnen, LLP
Wells Fargo Center
1248 O Street, Suite 600, Lincoln, NE 68508
Phone 402.475.1075 | Fax 402.475.9515
Syracuse Office
Phone 402.269.3200

However, if you were issued an identity theft letter, for example a 5071C or 4464C, follow the instructions on the letter and do not file the Form 14039 unless instructed to do so.

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 (402) 475-1075.

Baylor Evnen 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,

Jarrod P. Crouse
Managing Partner
Baylor Evnen, LLP
jcrouse@baylorevnen.com

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

File Your Tax Return. 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.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit http://www.taxadmin.org/state-tax-agencies.

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111 Or
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	1-800-349-9960
		www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

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, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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); 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 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 and your state Attorney General. This notice has not been delayed by law enforcement.