MKK
CONSULTING ENGINEERS, INC.

May 11, 2016

Dear,

The privacy of your personal information is of utmost importance to MKK Consulting Engineers, Inc. We are writing with important follow-up information about a recent incident involving the security of our employees' personal information. We wanted to provide you with additional information regarding the incident and explain the services we are making available to help safeguard you against identity fraud. We also are providing additional steps you can take to help protect your information. This letter is a follow up notification of the email notices sent to you on April 6, 7, and 19, 2016.

What Happened?

On April 6, 2016 we discovered that on February 19, 2016, as a result of a phishing email received by one of our employees appearing to come from MKK's President/CEO, an unauthorized third party received an electronic file containing certain information on current and former employees who received employment earnings in 2015 from MKK Consulting Engineers, Inc.

What Information Was Involved?

We have confirmed that the information sent to the unauthorized party included your 2015 W-2, which included your full name, Social Security number, home address, and earnings.

What We Are Doing

Upon learning of the issue, we promptly launched an investigation, including reporting the incident to law enforcement. As part of our investigation, we have been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents. While we cannot make a direct link to this incident, we are aware that some employees have recently experienced tax fraud issues. Out of an abundance of caution, we wanted to again make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps you should take.

What You Can Do

On April 7 and 19, 2016 you were provided with information on enrolling in a 12-month membership of IDShield/LegalShield at no cost to you. You also were provided other precautionary measures to help protect your personal information, which included: placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you also were notified you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

The information that is likely to be most at risk in this situation is the type of information that may be used to file fraudulent tax returns. As a result, you should contact your tax advisor, if you have one, and let them know that this information may be at risk. You should also file your tax return as quickly as possible, if you have not already done so.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax return electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you contact your tax advisor, if you have one; file an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf); call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and report the situation to your local police department. Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

As a reminder, always verify the email address and sender of any email you receive requesting confidential or sensitive information. If you have any doubt about a request for confidential information, you should contact the apparent requestor via telephone or in person to confirm the request.

For More Information

If you have any further questions regarding this incident, the information that was provided to you on April 6, 7, and 19, 2016, or the information contained in this letter, please call me at (303) 796-6060, during normal business hours.

On behalf of MKK Consulting Engineers, Inc., please accept our sincere apologies that this incident occurred. We continually evaluate and modify our practices to enhance the security and privacy of your information. Please know that we are devoting considerable resources to ensure our employees are fully informed as a result of this unfortunate incident.

Sincerely,

Kay M. Riley
Director of Corporate Operations
Principal

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3472

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
http://www.transunion.com/securityfreeze
1-800-680-7289

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

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

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

5. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

6. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf

MKK
CONSULTING ENGINEERS, INC.

May 11, 2016

Dear,

The privacy of your personal information is of utmost importance to MKK Consulting Engineers, Inc. We are writing with important follow-up information about a recent incident involving the security of our employees' personal information. We wanted to provide you with additional information regarding the incident and explain the services we are making available to help safeguard you against identity fraud. We also are providing additional steps you can take to help protect your information. This letter is a follow up notification information you received via Federal Express sent to you on April 8, and the same information that was sent to you again via certified mail on April 22, 2016.

What Happened?

On April 6, 2016 we discovered that on February 19, 2016, as a result of a phishing email received by one of our employees appearing to come from MKK's President/CEO, an unauthorized third party received an electronic file containing certain information on current and former employees who received employment earnings in 2015 from MKK Consulting Engineers, Inc.

What Information Was Involved?

We have confirmed that the information sent to the unauthorized party included your 2015 W-2, which included your full name, Social Security number, home address, and earnings.

What We Are Doing

Upon learning of the issue, we promptly launched an investigation, including reporting the incident to law enforcement. As part of our investigation, we have been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents. While we cannot make a direct link to this incident, we are aware that some employees have recently experienced tax fraud issues. Out of an abundance of caution, we wanted to again make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps you should take.

What You Can Do

On April 8 and 22, 2016 you were provided with information on enrolling in a 12-month membership of IDShield/LegalShield at no cost to you. You also were provided other precautionary measures to help protect your personal information, which included: placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you also were notified you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

The information that is likely to be most at risk in this situation is the type of information that may be used to file fraudulent tax returns. As a result, you should contact your tax advisor, if you have one, and let them know that this information may be at risk. You should also file your tax return as quickly as possible, if you have not already done so.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax return electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you contact your tax advisor, if you have one; file an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf); call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and report the situation to your local police department. Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

As a reminder, always verify the email address and sender of any email you receive requesting confidential or sensitive information. If you have any doubt about a request for confidential information, you should contact the apparent requestor via telephone or in person to confirm the request.

For More Information

If you have any further questions regarding this incident, the information that was provided to you on April 8, and 22, 2016, or the information contained in this letter, please call me at (303) 796-6060, during normal business hours.

On behalf of MKK Consulting Engineers, Inc., please accept our sincere apologies that this incident occurred. We continually evaluate and modify our practices to enhance the security and privacy of your information. Please know that we are devoting considerable resources to ensure our employees are fully informed as a result of this unfortunate incident.

Sincerely,

Kay M. Riley
Director of Corporate Operations
Principal

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3472

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
http://www.transunion.com/securityfreeze
1-800-680-7289

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

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

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

5. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

6. **Reporting Identity Fraud to the Social Security Administration.**

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf