



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

August 31, 2018

[Via email to DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov)
Attorney General Gordon MacDonald
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Potential Data Security Incident

Dear Attorney General MacDonald:

We represent TKC Holdings, Inc. (“TKC”) with respect to a recent data security incident described in greater detail below. TKC is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On May 24, 2018, TKC discovered unusual activity in its email system. TKC immediately took action to secure the email system and began an investigation. TKC retained an independent computer forensics expert to assist with the investigation, and the expert determined that an unauthorized individual accessed two TKC employees’ email accounts. On July 5, 2018, the investigation confirmed that personally identifying information belonging to some TKC employees in the email accounts was at risk. There is no evidence of the misuse of any information potentially involved in this incident, and TKC has notified the potentially affected population.

2. Number of New Hampshire residents affected.

A total of 1 resident of New Hampshire was affected by this incident. A notification letter was sent to this individual on August 24, 2018 via first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

TKC has taken steps in response to this incident to strengthen the security of personal information in its possession, in an effort to prevent similar incidents from occurring in the future. In addition,

potentially impacted individuals have been offered 12 months of identity protection services through Kroll, at no charge to the individual.

4. Contact information.

TKC remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141, or by e-mail at lindsay.nickle@lewisbrisbois.com.

Please let me know if you have any questions.

Best regards,



Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

KEC
Enclosure



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Data Security Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a data security incident that may have involved your personal information. At TKC Holdings, Inc. ("TKC") we take the privacy and security of our employees' information very seriously and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information and the resources we are making available to help you.

What Happened?

On May 24, 2018, we discovered unusual activity in our email system. Upon this discovery, we immediately began an investigation and took steps to secure our email system. We also engaged an independent computer forensics expert to help us determine the nature and scope of the incident. Through the investigation, we learned that an unauthorized individual accessed two TKC employee email accounts and may have viewed emails containing text or attachments that included your personal information. Please note, at this time, we are unaware of the misuse of any of your personal information.

What Information Was Involved?

The information potentially impacted by this incident may have included your name and/or Social Security number.

What we are doing and what you can do.

As stated above, we are not aware of the misuse of any personal information involved in this incident. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. 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, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit monitoring services by mail instead of online, please call 1-???-???-?????. Additional information describing your services is included with this letter.

In addition, to receive credit monitoring services, you must be over the age of 18, 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.

We also recommend that you review the enclosed information about steps you can take to protect your personal information and that you review your current and past financial account statements for discrepancies or unusual activity dating back to May 2018. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the account immediately.

For More Information.

If you have questions, please call 1-???-??-???, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

We sincerely regret any inconvenience or concern that this matter may cause you and remain dedicated to protecting all information in our systems.

Sincerely,

A handwritten signature in black ink, appearing to read "Khadeeja Morse", with a long horizontal flourish extending to the right.

Khadeeja M. Morse
Chief Human Resources Officer
TKC Holdings, Inc.

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 should also 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 (the "FTC").

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 also contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion	Free Annual Report
P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert 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. 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>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This 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. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov , and www.ftc.gov/idtheft 1-877-438-4338	200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

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'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

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.

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.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.