



Baker&Hostetler LLP

One North Wacker Drive
Suite 4500
Chicago, IL 60606-2841

T 312.416.6200
F 312.416.6201
www.bakerlaw.com

David H. Potter
direct dial: 312.416.6278
dpotter@bakerlaw.com

April 17, 2024

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Sir or Madam:

We are writing on behalf of our client, Tittmann Weix LLP ("TW"), to provide notice to your office concerning a security incident involving 1 Maryland resident.

On January 5, 2024, TW identified phishing emails being sent from one employee's email account. TW immediately took steps to secure the account involved and began an investigation. The investigation determined that an unauthorized party accessed the employee's email account at different times between October 8, 2023 and January 5, 2024. The investigation was unable to identify which, if any, emails or attachments were accessed or viewed by the unauthorized party. A team reviewed the emails and attachments from the account, and on February 15, 2024, determined that an email or attachment included the personal information of 1 Maryland resident, including the individuals' Driver's License number.

TW reviewed its records and determined that the Maryland resident is associated with one of TW's clients.¹ TW notified the client involved and offered to notify the Maryland resident on behalf of the client. On April 11, 2024, TW received instruction from the client to mail a notification letter to the Maryland resident.

¹ The data owner for the individuals involved is Assurant, Inc.

April 17, 2024

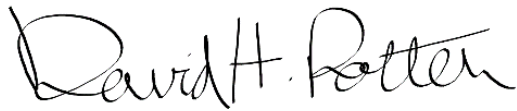
Page 2

On April 17, 2024, TW will mail a notification letter to the Maryland resident via First Class mail in accordance with Md. Code Ann., Com. Law § 14-3504.² A copy of the notification letter is attached. TW is providing the Maryland resident two years of credit monitoring and identity theft protection services through Kroll. TW has also established a dedicated, toll-free call center that individuals can call to obtain more information regarding the incident.

To help prevent a similar incident in the future, TW has implemented additional security measures, employee training and technical controls to enhance the security of its email environment.

Please do not hesitate to contact me if you have any questions regarding the matter.

Sincerely,

A handwritten signature in black ink that reads "David H. Potter". The signature is written in a cursive, flowing style.

David H. Potter
Counsel

Enclosure

² This report does not waive TW's objection that Maryland lacks personal jurisdiction over TW related to this matter.

TITTMANN|WEIX

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

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

<<b2b_text_1(Notice of Data Breach - CA Only)>>

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

TittmannWeix LLP (“TW”) is writing to inform you of an incident that involved some of your information. This notice explains the incident, the measures we have taken, and some additional steps you may consider taking in response.

What Happened? On January 5, 2024, we identified phishing emails being sent from one of our employee’s email accounts. We immediately took steps to secure the account involved and began an investigation. The investigation determined that an unauthorized party accessed an employee’s email account at different times between October 8, 2023 and January 5, 2024. The investigation was unable to identify which, if any, emails or attachments were accessed or viewed by the unauthorized party.

What Information Was Involved? A team reviewed the emails and attachments from the account, and on February 15, 2024, we determined that an email or attachment included your <<b2b_text_2(name, data elements)>>.

What We Are Doing? We assure you that we take this incident seriously. To help prevent a similar incident in the future, we have implemented additional security measures, employee training and technical controls to enhance the security of our email environment. Additionally, we have arranged to provide identity monitoring at no cost to you for two years through Kroll. The identity monitoring services we are making available to you include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention and Kroll Identity Monitoring, including instructions on how to activate your complimentary membership, please see the additional information provided with this letter.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

What You Can Do? For more information on Kroll Identity Monitoring, including instructions on how to activate your complimentary membership, as well as some additional steps you can take in response, please see the pages that follow this letter.

For More Information. We apologize for any concern this incident may cause you. If you have any questions regarding this notice, please call [TFN](tel:1800444444), Monday through Friday from 6:00 AM to 3:30 PM, Pacific Time, excluding certain major U.S. holidays.

Sincerely,

TittmannWeix LLP



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—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 will be able to help you determine if it is 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.

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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also 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. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

TittmannWeix is located at 350 S Grand Ave Suite 1630, Los Angeles, CA 90071, and can be reached by telephone at (213) 797-0630.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov