

Blair Dawson, JD, MS CyS, CIPP/US, CIPP/E, CIPM
Direct Dial: (312) 642-6131
E-mail: bdawson@mcdonaldhopkins.com

August 16, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: T&B Inc. – Incident Notification

Dear Attorney General Brown:

McDonald Hopkins PLC represents T&B Inc. (“T&B”). I am writing to provide notification of an incident at T&B that may affect the security of personal information of approximately 1 Maryland resident. T&B’s investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, T&B does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

T&B experienced a security incident on January 31, 2024. Upon learning of this issue, T&B immediately contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, T&B engaged external cybersecurity professionals experienced in handling these types of incidents to determine the extent of any compromise of the information on the T&B network. Based on the comprehensive investigation, T&B concluded that certain documents and records maintained within their possession were accessed and/or obtained in connection with this incident. Following the extensive manual document review, T&B determined on August 8, 2024, that certain personal information was present in those documents and records. The impacted data includes full name and address in combination with Social Security number, Financial Account Number with Password or Routing Number, Date of Birth, State Identification Number, Credit/Debit Card Number without Password or Security Code, Username and Password, Digital Signature, Health Insurance App/Claims Info, Medical History, Condition, Treatment, or Diagnosis. Not all data elements were impacted for every Maryland resident.

To date, T&B is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, T&B is providing notice to the affected clients commencing on August 16, 2024 in substantially the same form as the enclosed letter (Attached as Exhibit A). The notified individuals who have had their Social Security number impacted will receive complimentary credit monitoring services. Additionally, T&B will

August 16, 2024

Page 2

advise all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. T&B will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Protecting the privacy of personal information is a top priority for T&B. T&B remains fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. T&B continually evaluates and modifies practices to enhance the security and privacy of personal information.

Should you have any questions regarding this notification, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to be 'BLD', followed by a long horizontal flourish.

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM

Encl.

Exhibit A



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line



***IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY***

Dear [REDACTED]

I am writing with important information regarding a recent data security incident that T&B Inc. ("T&B") experienced. The privacy and security of the protected personal information entrusted to us is of the utmost importance to T&B. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that we experienced a security incident on January 31, 2024 where an unauthorized actor was able to access and exfiltrate certain files from within our network.

What We Are Doing.

Upon learning of the incident, we commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to help determine whether any sensitive data had been compromised. As part of our investigation, we notified the Federal Bureau of Investigation of the incident. After an extensive investigation and manual review of the impacted data, we discovered on August 8, 2024 that the files that were accessed by the unauthorized actor contained some of your protected personal information. We want to make you aware of the incident and provide you with steps you can take to protect your information further.

What Information Was Involved?

The data accessed by the unauthorized actor contained some of your protected personal information, including your name, address, [REDACTED]

What You Can Do.

We are providing you with complimentary access to Experian IdentityWorksSM for <<12/24>> months. An Experian Identity Restoration 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).

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary <<12/24>>-month 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 [REDACTED] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [REDACTED]
- Your activation code: [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED]. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

This letter also provides other precautionary measures to protect your personal information, including placing a fraud alert and/or security freeze on your credit files and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We sincerely regret the occurrence of this incident. We have always been committed to maintaining the proper handling, protection, and privacy of protected personal information in our possession and have taken precautions to safeguard it.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED] Representatives are available from 9:00 am to 9:00 pm Eastern Time, Monday through Friday, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information.

Sincerely,

Ralph Etter | President, Owner |
Eastside Equities, Inc.; T&B, Inc.; and WWCD Restaurants Inc.
230 Auburn Way South, Suite 2B Auburn, WA 98002-5451

– OTHER IMPORTANT INFORMATION –

1. Additional Details Regarding Your Experian IdentityWorks Membership.

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 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 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. 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 at no cost. 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 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888) 298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing 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.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. 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.

5. 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 TTY: 1-866-653-4261, 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.

You may also reach out to the Social Security Administration to notify them of the impact on your Social Security Number. They may be reached via the telephone by contacting the National 800 Number at 1-800-772-1213 between 8:00 a.m. – 7:00 p.m. Eastern Time, Monday through Friday. If you are deaf or hard of hearing and use TTY equipment, you can call the TTY number at 1-800-325-0778.

6. State Specific Information.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA) which include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.