JacksonLewis

Jackson Lewis P.C.
666 Third Avenue
New York NY 10017-4030
(212) 545-4000 Main
(212) 972-3213 Fax
jacksonlewis.com

DIRECT DIAL: (212) 545-4006
EMAIL ADDRESS: GREGORY.BROWN@JACKSONLEWIS.COM

June 30, 2023

VIA FIRST-CLASS MAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: ***Data Incident Notification***

Dear Sir or Madam:

We are writing to notify your office of a data security incident affecting one (1) New Hampshire resident. We are submitting this notice as counsel for Citarella Operating, LLC and Lockwood & Winant Seafood, LLC (collectively, "Citarella and Lockwood"), whose mailing address is 2135 Broadway, New York, NY 10023.

Citarella and Lockwood were subject to a ransomware attack on February 10, 2023 ("Incident"). With assistance from third-party experts, Citarella and Lockwood took immediate steps to secure their systems and investigate the nature and scope of the Incident. As part of Citarella and Lockwood's extensive investigation, they worked diligently to identify any personal information that may have been subject to unauthorized access or acquisition as a result of the Incident. Citarella and Lockwood have not found any evidence that personal information was misused as a result of the Incident.

On or about May 30, 2023, Citarella and Lockwood determined that the Incident may have impacted personal information related to one (1) New Hampshire resident. The categories of personal information involved in the Incident are [1]

Out of an abundance of caution, and in accordance with applicable law, Citarella and Lockwood will provide notice to the affected New Hampshire resident, in the form enclosed as Exhibit A, so that they can take steps to minimize the risk that their information will be misused. Additionally, Citarella and Lockwood have arranged for the individual to enroll in free credit monitoring and related services for

Citarella and Lockwood treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, Citarella and Lockwood have taken a number of steps to further secure their systems. Specifically, they have rebuilt all of the systems impacted by the Incident; have deployed endpoint detection and response within their environments and

[1] For the affected New Hampshire resident, only credit card information may have been impacted.

will continue to utilize this solution on a going forward basis; reset passwords; and thoroughly reviewed and upgraded their data security policies and procedures.

Citarella and Lockwood will continue to monitor this situation and will update you on any significant developments. If you require any additional information on this matter, please contact me.[2]

Sincerely,

JACKSON LEWIS P.C.

Gregory C. Brown, Jr.

Enclosure.

[2] Please note that Citarella and Lockwood are not, by submitting this letter, agreeing to the jurisdiction of State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

EXHIBIT “A”

Citarella . Lockwood & Winant

THE ULTIMATE GOURMET MARKET

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

June 30, 2023

Incident Notice

Dear <<First Name>> <<Last Name>>,

What Happened

We are writing to notify you that Citarella and Lockwood & Winant Seafood were subject to a ransomware attack on February 10, 2023 (the "Incident"). With assistance from third-party experts, we took immediate steps to secure our systems and investigate the nature and scope of the Incident. As part of our extensive investigation, we worked diligently to identify any personally identifiable information ("PII") that may have been subject to unauthorized access or acquisition as a result of the Incident. On or about May 30, 2023, we determined that the Incident may have impacted PII related to you. However, we have not found any evidence that your information was misused.

What Information Was Involved

The Incident may have impacted the following categories of PII related to you:

What We Are Doing

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we have arranged for Equifax to provide you of free credit monitoring and related services. To enroll, please visit www.equifax.com/activate or call Your enrollment code is <<Activation Code>>. To receive these services, please be sure to enroll by <<Enrollment Deadline>>.

We treat all sensitive information in a confidential manner and are proactive in the careful handling of such information. Since the Incident, we have implemented additional cybersecurity enhancements.

What You Can Do

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

For More Information

If you have questions or concerns, please call us at , Monday through Friday from 9:00 a.m. to 9:00 p.m., Eastern Time. We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

Helen Gurrera
President
Citarella

Nancy Pesola
Controller
Lockwood & Winant Seafood

What You Should Do To Protect Your Personal Information

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

   - Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
   - You can also receive information from these agencies about avoiding identity theft, such as by placing a "security freeze" on your credit accounts.
   - Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
   - Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	Databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a "security freeze" on your credit accounts. The FTC can be contacted either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement or the attorney general, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

4. *For District of Columbia Residents*: You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001, (202) 727-3400, www.oag.dc.gov.

5. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, marylandattorneygeneral.gov.

6. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

7. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

8. *For Rhode Island Residents:* You may contact and obtain information from and/or report identity theft to your state attorney general at:

Rhode Island Attorney General's Office
150 South Main Street
Providence, RI 02903
Phone: (401) 274-4400
Website: www.riag.ri.gov

You have the right to obtain a copy of the applicable police report, if any, relating to this incident. You may want to place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, please follow these instructions:

- Equifax:
  https://www.equifax.com/personal/credit-report-services/credit-freeze/

- Experian:
  https://www.experian.com/freeze/center.html

- Transunion:
  https://www.transunion.com/credit-freeze

Mailing addresses for the credit reporting agencies are provided above. Credit reporting agencies may charge a $5.30 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft, in which case there is no fee. A copy of your police report or an investigative report or written FTC complaint documenting identity theft must be included to avoid a fee. In your request, you also must include: (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth; (iii) if you have moved in the past five years, the address of each residence you lived at during that time period; (iv) proof of current address, such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable, (vi) payment by check, money order, or credit card (Visa, Master Card, American Express, or Discover cards only.)

You can also place a fraud alert with the credit reporting agencies. This will flag your file with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit. To place a fraud alert on your credit file call the fraud department of one of the three credit reporting agencies – Experian, Equifax, or TransUnion (see above). When you request a fraud alert from one agency, it will notify the other two for you. You can place an initial fraud alert for 90 days, and may cancel the fraud alerts at any time.