McDonald Hopkins
A business advisory and advocacy law firm®

RECEIVED
JUN 18 2020
CONSUMER PROTECTION

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Christine N. Czuprynski
Direct Dial: 248-220-1360
E-mail: cczuprynski@mcdonaldhopkins.com

June 15, 2020

VIA U.S. MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Orascom Construction USA, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Orascom Construction USA, Inc. I am writing to provide notification of an incident at Orascom Construction USA, Inc. and its operating entities The Weitz Company, LLC; Contrack-Watts, Inc.; and Watts Constructors, LLC (hereinafter "Orascom") that may affect the security of personal information of one (1) New Hampshire resident. Orascom's investigation is ongoing, and this notification will be supplemented with new or significant facts or findings subsequent to this submission, if any. By providing this notice, Orascom does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Orascom learned that an employee email account may have been compromised as a result of a phishing attack. The incident resulted in unauthorized access to that email account. Upon learning of the issue, Orascom immediately secured the account and commenced a prompt and thorough investigation. The extensive forensic investigation reviewed all email accounts for possible unauthorized access to ensure that the nature and scope of the incident was known. Following the comprehensive investigation and subsequent manual email review, Orascom discovered on May 4, 2020 that the incident impacted two email accounts. Those two accounts were accessed between January 15, 2019 and February 8, 2019 and contained personal information. Orascom has no evidence that any of the information has been misused. The impacted data includes the affected resident's name, Social Security Number, and health insurance information.

Out of an abundance of caution, Orascom wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the impacted resident against identity fraud. Orascom is providing the affected resident with written notification of this incident commencing on or about June 8, 2020 in substantially the same form as the letter attached hereto. Orascom is offering the resident a one-year membership in credit monitoring services at its own expense in order to protect them against identity theft. Orascom is

also advising the affected resident about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Orascom, protecting the privacy of personal information is a top priority. Since learning of the incident, Orascom has implemented enhanced security safeguards to help protect against similar intrusions. Orascom is also conducting ongoing monitoring of its network to ensure that it is secure and cleared of any malicious activity.

Should you have any questions concerning this notification, please contact me at (248) 220-1360 or cczuprynski@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Christine N. Czuprynski

Encl.

ORASCOM CONSTRUCTION | USA

WEITZ CONTRACK WATTS WATTS

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
[redacted]
Or Visit:
[redacted]
Enrollment Code: [redacted]

[redacted]

[redacted]

Dear [redacted]:

We are writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to Orascom Construction USA, Inc. and its operating entities The Weitz Company, LLC; Contrack-Watts, Inc.; and Watts Constructors, LLC. 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?

An employee email account may have been compromised as a result of a phishing attack. The incident resulted in unauthorized access to that email account.

What We Are Doing?

Upon learning of the issue, we immediately commenced a prompt and thorough investigation and contained the compromised account. As part of our extensive investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The extensive forensic investigation reviewed all of our email accounts for possible unauthorized access to ensure that the nature and scope of the incident was known.

What Did We Discover?

Following the comprehensive investigation and subsequent manual email review, we discovered that the incident impacted two of our email accounts. The identities of those two email accounts will not be shared due to privacy concerns. Those two accounts were accessed between January 15, 2019 and February 8, 2019 and we believe may have contained some of your personal information. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What Information Was Involved?

On May 4, 2020, we learned that the impacted email accounts contained some of your personal information, specifically your [redacted]

What You Can Do?

To protect you from further misuse of your information, we are offering identity theft protection services through ID Experts® that offers MyIDCare™. The MyIDCare services include 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. For more information on identity theft prevention and MyIDCare, including instructions on how to activate your free one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take 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 account statements for fraudulent or irregular activity on a regular basis. To the extent it is helpful, we have also provided information on protecting your medical information on the following pages.

For More Information.

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

Sincerely,

Orascom Construction USA, Inc.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

We encourage you to contact ID Experts to enroll in the free MyIDCare services by calling [redacted] or going to [redacted] and using the enrollment code provided below. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 8, 2020.

The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

- **To Enroll:** Please call [redacted] or visit [redacted] and follow the instructions for enrollment using your Enrollment Code provided below.

  Enrollment Code: [redacted]

Contact MyIDCare at [redacted] to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you have any reason to suspect that you might be the victim of identity theft and have enrolled in MyIDCare, notify MyIDCare immediately by calling or by logging into the MyIDCare website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of the ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year "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	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. 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 charge*. 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 or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-888-909-8872

In order to place the security freeze, 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 monitoring 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 your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

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 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.

6. Protecting Your Medical Information.

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.