

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

June 15, 2020

VIA EMAIL (consumer@ag.iowa.gov)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

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 seven hundred fifty-six (756) Iowa residents. 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 Iowa 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 residents’ Social Security Numbers; driver license numbers or other unique identification numbers; medical treatment information, health insurance information, and/or financial account number or credit card number or debit card number.

Out of an abundance of caution, Orascom wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the impacted residents against identity fraud. Orascom is providing the affected residents with written notification of this incident commencing on or about June 8, 2020 in substantially the same form

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
June 15, 2020
Page 2

as the letter attached hereto. Orascom is offering all the Iowa residents whose SSNs were impacted 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 residents about the process for placing fraud alerts and/or security freezes 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, the Iowa attorney general's office, 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,



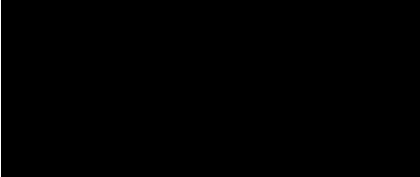
Christine N. Czuprynski

Encl.



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

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



**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**



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; Contract-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

P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC

P.O. Box 2000
Chester, PA 19016
www.transunion.com
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

P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
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.

If this notice letter states that your financial account information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: (515) 281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These 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 about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-775 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

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.