

James J. Giszczak
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

January 23, 2018

Office of Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Insight Sourcing Group Holdings, LLC (“Insight Sourcing”). I write to provide notification concerning an incident at Insight Sourcing. This incident may affect the security of personal information of one (1) Washington resident who is an Insight Sourcing employee. Insight Sourcing’s investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, Insight Sourcing does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

Insight Sourcing recently learned that a limited number of email users within Insight Sourcing Group & SpendHQ were victims of a criminal phishing attack. On January 4, 2018, Insight Sourcing learned that the phishing attack resulted in unauthorized access to one user’s email box from approximately November 30, 2017 through December 11, 2017. As a result, an unknown individual may have had access, via that compromised email account, to personal information belonging to employees.

The unauthorized party was potentially able to access personal information of the Washington resident, including name, address, date of birth, and Social Security number.

To date, Insight Sourcing has not received any reports of identity fraud, theft or specific misuse of information as a direct result of this incident. Nevertheless, we wanted to make you (and the potentially affected resident) aware of the incident and explain the steps that have been taken to date. The Washington resident impacted by this incident was provided with written notice commencing on January 23, 2018, in substantially the same form as the notice attached hereto. The residents may contact Insight Sourcing with questions regarding the incident.

Insight Sourcing will offer two (2) years of complimentary credit monitoring services to the affected individuals whose Social Security numbers were compromised. Insight Sourcing will advise the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Insight Sourcing will advise the residents about the process for

Washington Department of Justice
Office of the Attorney General
January 23, 2018
Page 2

placing a fraud alert on credit files, placing a security freeze, and obtaining a free credit report. The residents will be provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Insight Sourcing takes its obligation to help protect personal information very seriously and continually evaluates and modifies its practices to enhance appropriate security and privacy measures.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

A handwritten signature in blue ink, appearing to read "James J. Giszczak".

James J. Giszczak

Encl.

Tuesday, January 23, 2018

IMPORTANT INFORMATION

PLEASE READ CAREFULLY

«Full_Name»
«Address_1»
«Address_2»
«City», «State» «Zip»

Dear «Full_Name»,

The privacy of your personal information is of utmost importance to Insight Sourcing Group & SpendHQ. We are writing to provide you important information about a recent incident which involves the security of some of your personal information. We want to provide you information regarding the incident and explain the services we are making available to help safeguard you against identity fraud. We also are providing additional steps you can take to help protect your information.

What Happened?

We recently learned that a limited number of email users within Insight Sourcing Group & SpendHQ were victims of a criminal phishing attack resulting in unauthorized access to those users' email boxes from approximately November 30, 2017 through December 11, 2017.

What We Are Doing.

Upon learning of the issue, we promptly responded to the incident, reset log-in credentials and implemented multi-factor authentication for all email accounts. In addition, an independent cybersecurity forensic firm was engaged to analyze the incident and the extent of any compromise to the email accounts.

What Information Was Involved?

Although the comprehensive forensic investigation is ongoing, we believe that an unauthorized third party may have had access to an email containing names, addresses, date of births, and Social Security numbers.

What You Can Do.

To protect you from potential misuse of your information we are offering a complimentary two-year membership of identity theft protection and credit monitoring services through TransUnion. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.

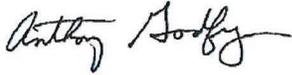
Also enclosed you will find other precautionary measures you can take to protect your personal information, including obtaining a free credit report and placing a Fraud Alert and/or Security Freeze on your credit files. You should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

For More Information.

We are committed to maintaining the privacy of our employees' personal information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of information.

If you have any further questions regarding this incident, please call me at 770-481-3030.

Sincerely,

A handwritten signature in black ink that reads "Anthony Godfrey". The signature is written in a cursive style with a large, stylized initial "A".

Anthony Godfrey
Insight Sourcing Group & SpendHQ

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 2 Years Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following 12-letter Activation Code: **«Activation Code»** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code **697885** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **April 30, 2018**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 2 year 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
www.equifax.com
1-800-525-6285

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

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

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. 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

PO Box 105788
Atlanta, GA 30348

<https://www.freeze.equifax.com>

1-800-685-1111

Experian Security Freeze

PO Box 9554
Allen, TX 75013

<http://experian.com/freeze>

1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19022

<http://www.transunion.com/securityfreeze>

1-800-680-7289

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.

McDonald Hopkins

A business advisory and advocacy law firm®

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



Office of Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

981043188 0022