McDonald Hopkins
A business advisory and advocacy law firm

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

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

July 13, 2018

Office of the Washington State Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: ComplyRight, Inc.

Dear Sir or Madam:

McDonald Hopkins PLC represents ComplyRight, Inc. ("ComplyRight"). I write to provide notification concerning an incident that may affect the security of personal information of twenty nine thousand three hundred twenty two (29,322) Washington residents. ComplyRight'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, ComplyRight does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

ComplyRight maintains web platforms for entity users and employers to prepare tax related forms, such as 1099s and W-2s for employees and independent contractors. ComplyRight does not do business directly with the individual tax form recipients. Rather, ComplyRight does business with some of the users of its web platform; some users directly access a ComplyRight website while other users access a website of a reseller of ComplyRight's web platform. Out of abundance of caution, however, ComplyRight provided notice to all affected individuals, as well as site users and payers.

On or about May 22, 2018 ComplyRight initially learned of a potential issue involving its website. Upon learning of the potential issue, ComplyRight disabled the platform and remediated the issue on the website. In addition, ComplyRight commenced a prompt and thorough investigation using external cybersecurity professionals. The forensic investigation concluded that there was unauthorized access to ComplyRight's website, which occurred between April 20, 2018 and May 22, 2018. After the extensive forensic investigation, a sophisticated review of its website, and analysis of potentially impacted individuals, on June 14, 2018 ComplyRight discovered that some personal information was accessed and/or viewed.

Although the forensic investigation determined that individual information was accessed and/or viewed, it could not confirm if the information was downloaded or otherwise acquired by

an unauthorized user. ComplyRight confirmed that the personal information that was accessed and/or viewed on the website, and may have been downloaded or otherwise acquired by an unauthorized user, included name, address, telephone number, email address, and Social Security number of a portion of the individual tax form recipients.

To date, ComplyRight is not aware of any instances of identity fraud as a direct result of this incident. Nevertheless, ComplyRight wanted to make you (and the affected residents) aware of the incident and explain the steps ComplyRight is taking to help safeguard the residents against identity fraud. ComplyRight provided the residents with written notice of this incident commencing on July 13, 2018, in substantially the same form as the letter attached hereto. ComplyRight is offering the residents a complimentary membership with a credit monitoring and identity theft protection service. ComplyRight will provide dedicated call center support to answer questions. ComplyRight has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. ComplyRight has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and obtaining a free credit report. The residents also have been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

ComplyRight takes this situation very seriously and regrets any inconvenience or concern this incident may cause individuals. Maintaining the integrity of personal information is of the utmost importance to ComplyRight, and, moving forward, ComplyRight is taking steps to strengthen its security protocols and practices to help prevent similar issues in the future.

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

Sincerely,

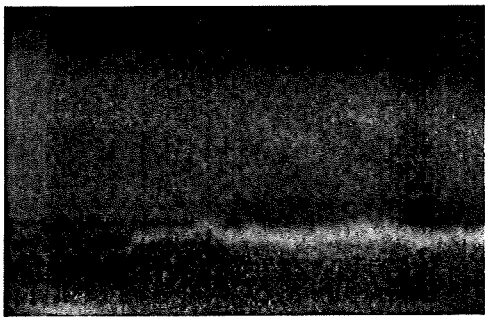
James J. Giszczak

COMPLYRIGHT

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

IMPORTANT INFORMATION

PLEASE READ CAREFULLY



[redacted]

Dear [redacted]

The privacy and security of your personal information is of the utmost importance to ComplyRight, Inc. ("ComplyRight"). We are writing with important information about a recent security incident involving some of your personal information that was maintained on our website. Your personal information was entered onto our website by, or on behalf of, your employer or payer to prepare tax related forms, for example, Forms 1099 and W-2. We wanted to provide you with information regarding the incident, share the steps we have undertaken since discovering the incident, and provide guidance on what you can do to protect yourself.

What Happened?

On or about May 22, 2018 we initially learned of a potential issue involving our website. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website.

What We Are Doing.

In addition, we commenced a prompt and thorough investigation using external cybersecurity professionals. The forensic investigation concluded that there was unauthorized access to our website, which occurred between April 20, 2018 and May 22, 2018. After the extensive forensic investigation, a sophisticated review of our website, and analysis of potentially impacted individuals, on June 14, 2018 we discovered that some of your personal information was accessed and/or viewed. Although the forensic investigation determined that your information was accessed and/or viewed on the website, it could not confirm if your information was downloaded or otherwise acquired by an unauthorized user. We are not aware of any reports of identity fraud as a direct result of this incident. Nevertheless, out of an abundance of caution, we wanted to make you aware of the incident.

What Information Was Involved?

Your personal information that was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user included your name, address, telephone number, email address, and Social Security number.

What You Can Do.

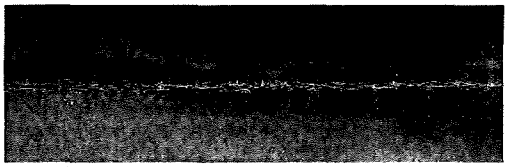
To protect you from potential misuse of your information we are providing you with 12 months of free credit monitoring and identity theft protection services through TransUnion. This service helps detect possible misuse of your personal information and provides you with identity protection services focused 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 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, placing a Security Freeze, 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.

Please know that we take this situation very seriously and regret any inconvenience or concern this incident may cause you. Maintaining the integrity of your personal information is of the utmost importance to us, and, moving forward, we are taking steps to strengthen our security protocols and practices to help prevent similar issues in the future.

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]. 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 a.m. to 9 p.m. Eastern Time.

Sincerely,



COMPLYRIGHT, INC.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring and Identity Protection Services.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year 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 [redacted] and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [redacted] 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, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] 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 [redacted] 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 one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, 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.)

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month 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. Alternatively, you may file the Fraud Alert online. Here is a link to the Experian fraud alert home page: https://www.experian.com/fraud/center.html

Equifax	Experian	**TransUnion LLC**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

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

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze (FVAD)
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
https://freeze.transunion.com/

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

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 will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

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;
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; and
4. Payment of a fee, if applicable.

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.

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 https://www.identitytheft.gov/, by phone at 1-877-IDTHEFT (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.

Iowa Residents: You may obtain information about identity theft to local law enforcement or the Iowa Attorney General: Office of the Iowa Attorney General, Consumer Protection Division, 1305 East Walnut Street, Des Moines, IA 50319, (515) 281-5164, 1-888-777-4590, Fax: (515) 281-6771, www.iowaattorneygeneral.gov.

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.

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.