

McDonald Hopkins

A business advisory and advocacy law firm®

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

STATE OF NH
DEPT OF JUSTICE
2016 MAY 31 PM 3:21

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

May 19, 2016

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Single Digits – Incident Notification

Dear Attorney General Delaney:

We represent Single Digits and are writing to notify you of a data privacy incident at Single Digits that has affected the security of personal information of one hundred and eighty seven (187) New Hampshire residents. Single Digits' investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission. By providing this notice, Single Digits does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On May 17, 2016, Single Digits fell victim to a phishing email purportedly coming from its chief executive officer. As a result, an unauthorized third party was emailed an electronic file containing certain information on individuals that were employed by Single Digits during 2015. Upon learning of the issue, Single Digits' incident response team promptly began an investigation, engaged cybersecurity professionals to assist them, and took steps to prevent further unauthorized access to employee records. To date, they are not aware of any instances of identity fraud as a result of this incident.

Single Digits can confirm that the following information was emailed to the unauthorized third party: 2015 W-2 and Form 1095-C, which included your residents' full name, Social Security number, home address, and wage and tax information. The information did not contain any information related to spouses or dependents. As a result, we wanted to make you (and the affected residents) aware of the incident and explain the steps we are taking to safeguard against identity fraud.

Single Digits provided the New Hampshire residents with written notice of this incident commencing on May 19, 2016, in substantially the same form as the letter attached hereto. Single Digits has advised the residents to monitor all credit reports and bank statements. Single Digits has offered a complimentary two-year membership in Equifax Credit Watch™ Silver to all affected residents. Single Digits is also providing a direct telephone number for additional

Attorney General Michael A. Delaney

May 19, 2016

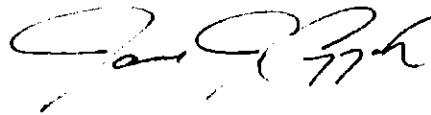
Page 2

support to those affected. Single Digits also advised the individuals affected to obtain a credit report and the process for placing a fraud alert on their credit files. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Maintaining the privacy of personal information is of the utmost importance to Single Digits. In light of this incident, Single Digits continues to monitor system activity and has implemented further security awareness for employees. Single Digits is also evaluating additional technical safeguards.

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

Sincerely,

A handwritten signature in black ink, appearing to read "James J. Giszczak". The signature is fluid and cursive, with a large initial "J" and "G".

James J. Giszczak

JJG/kjb

Encl.

Single Digits, Inc.
4 Bedford Farms
Bedford, NH 03110



**IMPORTANT INFORMATION
PLEASE READ CAREFULLY**

<<Date>>

FirstName LastName
Address1
Address2
City, State ZIP

Dear FirstName,

The privacy of your personal information is of utmost importance to Single Digits. I am writing with important information about a recent incident involving the security of our employees' personal information. We wanted to provide you with information regarding the incident and explain the services we are making available to help safeguard you against identity fraud.

What Happened?

On May 17, 2016, as a result of a phishing email purportedly coming from the chief executive officer, an unauthorized third party was emailed an electronic file containing certain information on individuals that were employed by Single Digits during 2015.

What Information Was Involved?

We have confirmed that the information obtained by the unauthorized party included your 2015 W-2 and Form 1095-C, which included your full name, Social Security number, home address, and wage and tax information. The information did not contain any information related to spouses or dependents.

What We Are Doing.

Upon learning of the issue, our incident response team promptly began an investigation, engaged cybersecurity professionals to assist us, and took steps to prevent further unauthorized access to employee records. **To date, we are not aware of any instances of identity fraud as a result of this incident.** However, out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps you should take.

Single Digits, Inc.
4 Bedford Farms
Bedford, NH 03110



What You Can Do.

Enclosed in this letter you will find information on enrolling in a 24-month membership of Equifax Credit Watch™ Silver, that we are providing at no cost to you, along with 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 for fraudulent or irregular activity on a regular basis.

The information that was obtained by the unauthorized third party, your W2 and Form 1095-C, is the type of information that may be used to file fraudulent tax returns. As a result, you should contact your tax advisor, if you have one, and let them know that this information may be at risk. You should also file your tax return as quickly as possible, if you have not already done so.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax return was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you contact your tax advisor, if you have one; file an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>); call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and report the situation to your local police department. Additional information regarding preventing tax related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>

As a reminder, always verify the email address and sender of any email you receive requesting confidential or sensitive information. If you have any doubt about a request for confidential information, you should contact the apparent requestor via telephone or in person to confirm the request.

For More Information.

If you have any further questions regarding this incident, please call Shannon Hathaway, Director of Human Resources, at (603) 580.1539 during normal business hours.

On behalf of Single Digits, please accept my sincere apology that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information, and have taken steps to prevent further unauthorized access to employee records.

Sincerely,

Bob Goldstein
Chief Executive Officer
Single Digits

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. **Enrolling in Complimentary 24-Month Credit Monitoring.**

Protecting your personal information is important to Single Digits. In response to this incident and as a precautionary measure, we have arranged with Equifax Personal Solutions to help you protect your identity and your credit information for two years, at no cost to you.

Equifax Credit Watch™ Silver will provide you with an “early warning system” to changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- o Comprehensive credit file monitoring of your Equifax credit report with daily notification of key changes to your credit file.
- o Wireless alerts and customizable alerts available
- o One copy of your Equifax Credit Report™
- o \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- o 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- o 90 day Fraud Alert placement with automatic renewal functionality *

To sign up online for online delivery go to www.myservices.equifax.com/silver. You must sign up for this credit monitoring before August 18, 2016. You will not be able to enroll after this date.

1. **Welcome Page:** Enter the following Activation Code in the “Activation Code” box and click the “Submit” button: XXXXXXXXXXXXX
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

† Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

This product is not intended for minors (under 18 years of age).

The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 24 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.

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 19022
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

Single Digits, Inc.
4 Bedford Farms
Bedford, NH 03110



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. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>
- Call the IRS at (800) 908-4490, ext 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>