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
E-mail: jgiszczak@mcdonaldhopkins.com

October 9, 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: Cedar County, Iowa Board of Supervisors – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents the Board of Supervisors for Cedar County, Iowa ("Cedar County"). I am writing to provide a voluntary notification of an incident at Cedar County that may affect the security of personal information of approximately four hundred and ninety-three (493) Iowa residents. Two-hundred seventeen (217) of these individuals are being notified under HIPAA and Cedar County has reported to OCR, while the remainder are being notified under Iowa state law. Despite the fact that we are notifying fewer than five hundred (500) Iowa residents, we wanted to voluntarily notify you of this event in the spirit of our relationship. Cedar County's investigation is ongoing, and this communication will be supplemented with any new or significant facts or findings subsequent to this submission, if any.

Cedar County was the target of an email phishing campaign that resulted in an unauthorized individual gaining access to a limited number of Cedar County employee email accounts. Upon learning of the issue, Cedar County secured the accounts and commenced a prompt and thorough investigation. As part of that investigation, Cedar County has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual email review, Cedar County discovered on September 10, 2020 that the email accounts that were accessed between August 18, 2019 and December 3, 2019 contained personal information of the affected residents' including Social Security numbers, driver's license numbers or state ID card numbers, financial account numbers, credit or debit card information, and biometric information.

To date, Cedar County has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, Cedar County wanted to inform you (and the affected residents) of the incident and to explain the steps it is taking to help safeguard the affected residents against identity fraud. Cedar County is providing the affected residents with written notification of this incident commencing on or about October 8, 2020 in substantially the

same form as the letter attached hereto. Cedar County is offering the affected residents whose Social Security numbers were impacted complimentary one-year memberships with a credit monitoring service. Cedar County is 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 Federal Trade Commission, and the Iowa Attorney General.

At Cedar County, protecting the privacy of personal information is a top priority. Cedar County is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Cedar County continually evaluates and modifies its practices to enhance the security and privacy of the personal information.

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

Very truly yours,

James J. Giszczak

Encl.

[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 the Cedar County Board of Supervisors ("Cedar County"). 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?

We recently learned that, as a result of a phishing incident, an unauthorized party obtained access to a limited number of Cedar County employee email accounts.

What We Are Doing.

Upon learning of the issue, we secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual email review, we discovered on September 10, 2020 that the email account that was accessed between August 18, 2019 and December 3, 2019 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?

The accessed account(s) contained some of your personal information, including your full name and [redacted].

What You Can Do.

To protect you from potential misuse of your information, we are offering you a complimentary one-year membership in LifeLock Defender™ Preferred identity theft protection provided by NortonLifeLock. For more information on identity theft prevention and LifeLock Defender™ Preferred, including instructions on how to activate your 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.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal 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, [redacted]

Sincerely,

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Cedar County has retained **NortonLifeLock** to provide one year of complimentary **LifeLock Defender™ Preferred** identity theft protection.

To activate your membership online and get protection at no cost to you:

1. [redacted] button (*do not attempt registration from a link presented by a search engine).*
2. You will be taken to another page where, [redacted] you may enter the **Promo Code:** [redacted] and click [redacted]
3. On the next screen, enter your **Member ID:** [redacted] and click [redacted]
4. Your complimentary offer is presented. Click the red [redacted] button.
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

Alternatively, to activate your membership over the phone, please call: [redacted]

You will have until [redacted] to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Defender™ Preferred** membership includes:

- ✓ Primary Identity Alert System†
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring**
- ✓ Norton™ Security Deluxe[2] (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to $25,000†††
- ✓ Personal Expense Compensation up to $25,000†††
- ✓ Coverage for Lawyers and Experts up to $1 million†††
- ✓ U.S-based Identity Restoration Team
- ✓ Annual Three-Bureau Credit Reports & Credit Scores[1]**
  The credit scores provided are VantageScore 3.0 credit scores based on Equifax, Experian and TransUnion respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.
- ✓ Three-Bureau Credit Monitoring[1]**
- ✓ USPS Address Change Verification Notifications
- ✓ Fictitious Identity Monitoring
- ✓ Credit, Checking and Savings Account Activity Alerts†**

[1]If your plan includes credit reports, scores, and/or credit monitoring features ("Credit Features"), two requirements must be met to receive said features: (i) your identity must be successfully verified with Equifax; and (ii) Equifax must be able to locate your credit file and it must contain sufficient credit history information. IF EITHER OF THE FOREGOING REQUIREMENTS ARE NOT MET YOU WILL NOT RECEIVE CREDIT FEATURES FROM ANY BUREAU. If your plan also includes Credit Features from Experian and/or TransUnion, the above verification process must also be successfully completed with Experian and/or TransUnion, as applicable. If verification is successfully completed with Equifax, but not with Experian and/or TransUnion, as applicable, you will not receive Credit Features from such bureau(s) until the verification process is successfully completed and until then you will only receive Credit Features from Equifax. Any credit monitoring from Experian and TransUnion will take several days to begin after your successful plan enrollment.
No one can prevent all identity theft or cybercrime. † LifeLock does not monitor all transactions at all businesses.
[2] Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.
**These features are not enabled upon enrollment. Member must take action to get their protection.
††† Reimbursement and Expense Compensation, each with limits of up to $25,000 for Defender Preferred. And up to $1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

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 and/or credit or debit card 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.