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

Dominic A. Paluzzi
Direct Dial: 248.220.1356
E-mail: dpaluzzi@mcdonaldhopkins.com

August 24, 2023

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: Greg Penning & Co., LLC – Incident Notification

To Whom This May Concern:

McDonald Hopkins PLC represents Greg Penning & Co., LLC ("Greg Penning"). I am writing to provide notification of an incident that may affect the security of personal information of five hundred and fifty-six (556) Iowa residents. Greg Penning's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Greg Penning does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

As a result of a security incident on October 31, 2022, an unauthorized party potentially accessed and acquired a limited number of Greg Penning documents. Upon learning of this issue, Greg Penning immediately began effort to remediate the issue and commenced a prompt and thorough investigation. As part of this investigation, Greg Penning has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Greg Penning devoted considerable time and effort to determine what information was contained in the potentially impacted documents. Based on this comprehensive investigation and manual document review, Greg Penning discovered on July 11, 2023 that the potentially impacted documents contained a limited amount of personal information, including the affected residents' full names, Social Security numbers driver's license numbers, financial account information, credit card account information, and health insurance information. Not all data elements were impacted for each resident.

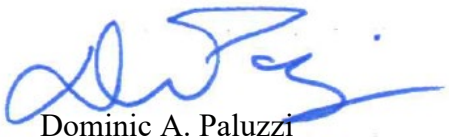
At the time of this notification, Greg Penning is not aware of any reports of identity theft or fraud arising out of this incident. Nevertheless, out of an abundance of caution, Greg Penning wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Greg Penning is providing the affected residents with written notification of this incident commencing on or about August 24, 2023 in substantially the same form as the letter attached hereto. Greg Penning is providing the affected residents with 12 months of complimentary credit monitoring services and will advise the affected residents to always remain vigilant in reviewing financial account statements

for fraudulent or irregular activity on a regular basis. Greg Penning will advise the affected residents about the process for placing a fraud alert and/or security freeze 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 and the Federal Trade Commission.

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

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,



Dominic A. Paluzzi

DAP/bg
Enclosure

[redacted]

GREG PENNING & CO. LLC
CERTIFIED PUBLIC ACCOUNTANTS

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

[redacted]

[redacted]

[redacted]

Dear [redacted]

Greg Penning & Co., LLC provides accounting-related services to businesses, including [redacted], and has access to certain personal information as a result. 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 Greg Penning & Co., 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?

As a result of a security incident on October 31, 2022, an unauthorized party potentially accessed and acquired a limited number of Greg Penning & Co., LLC documents.

What We Are Doing.

Upon learning of this issue, we immediately commenced a prompt and thorough investigation and took steps to contain the incident. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, we discovered on July 11, 2023 that some of your personal information was contained in the potentially impacted documents. Although we have no indication or evidence that any of that information has been misused, we wanted to make you aware of the incident.

What Information Was Involved?

The potentially impacted documents contained your [redacted].

What You Can Do.

We have no evidence that any of your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are offering a complimentary one-year membership in identity theft protection services through IDX. IDX identity protection 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, IDX will help you resolve issues if your identity is compromised. For more information on identity theft prevention and IDX identity protection services 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 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 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 [redacted]

Sincerely,

Greg Penning & Co., LLC
119 E. Call Street
Algona, IA 50511

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Go to [redacted] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Please note that the enrollment deadline is [redacted]

Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

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 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(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.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

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

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(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.

6. Reporting Identity Fraud to the IRS.

As noted above, 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), it is recommended that you do the following:

- **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)**
    - This form gets mailed or faxed to the IRS: Internal Revenue Service, Fresno, CA 93888-0025; 855-807-5720
    - ***Please note that this form should be used *only* if your Social Security number has been compromised and the IRS has informed you that you may be a victim of tax-related identity fraud or your e-file return was rejected as a duplicate.**
- 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 ET); and/or
- You may call or visit your local law enforcement agency and file a police report. Please bring this notice with you.

Additional information regarding preventing tax-related identity theft can be found at: http://www.irs.gov/uac/Identity-Protection. For further information and guidance from the IRS about tax-related identity theft, please visit: https://www.irs.gov/uac/taxpayer-guide-to-identity-theft (Taxpayer Guide to Identity Theft) and https://www.irs.gov/pub/irs-pdf/p5027.pdf (IRS Publication 5027, Identity Theft Information for Taxpayers).

7. Reporting Identity Fraud to the Social Security Administration.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess to block electronic access to your Social Security record. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf. This publication provides additional information on the potential impact of identity theft to your Social Security number and what actions you should take.