1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

**www.fmglaw.com**

**Nicholas Jajko**
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

June 1, 2022

**Via E-Mail Reporting**
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

**Re: DGN, LLC d/b/a Dennis, Gartland & Niergarth ("DGN") – Notice of Data Event**

Dear Sir or Madam:

We represent DGN, LLC d/b/a Dennis, Gartland & Niergarth ("DGN"), a full-service accounting firm based in Traverse City, Michigan. DGN is reporting to your Office on behalf of its client, Au Sable Institute of Mancelona, Michigan and makes this submission pursuant to the Maryland Personal Information Protection Act, MD. CODE ANN. COM. LAW §14-3501, et seq, which requires notice to your Office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

On March 14, 2022, DGN learned that its organization was the victim of a computer malware incident. Upon discovery, DGN immediately shut down its network and commenced an investigation that included partnering with cyber security incident specialists to secure and fully restore its systems safely. DGN reported the incident to the IRS and the Federal law enforcement. DGN determined that certain client files were obtained from its systems by someone outside the DGN organization. Though it cannot confirm with certainty, however, when the access began, or the full extent of which files were viewed or obtained by the unauthorized person. DGN knows that because some files within the affected systems contained individuals' personal information, it is possible the unauthorized person viewed or obtained that information. Therefore, DGN performed a review of its internal records that concluded on March 28, 2022, and has now notified potentially affected individuals and data owner clients of this incident out of an abundance of caution. The types of personal information impacted can include their name, address, and potentially other sensitive information such as a Social Security number, driver's

license/state identification number, date of birth, direct deposit financial information, and/or a passport or other secondary form of identification.

On or about April 29, 2022, DGN notified data owner clients, including Au Sable Institute, of the incident and thereafter received authorization to notify impacted individuals and report to applicable regulators on the data owner client's behalf. On or about June 1, 2022, DGN provided, via U.S. regular mail, notice of the incident to potentially impacted individuals for whom DGN was expressly authorized to do so. A sample copy of the notice letter is attached as "Exhibit A" for your records. DGN provided this notification to one (1) resident of Maryland.

DGN is providing written notice of the event to the potentially affected individuals that includes a brief description of the incident, encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements & credit reports, and immediately reporting errors or suspicious activity to the financial institution or issuing bank, and to file a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. DGN is offering twelve (12) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services through IDX. DGN also enclosed documentation containing contact information for the major consumer reporting bureaus, state-specific regulators, a 24-hour call center, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so.

After discovering the incident, DGN reset account and system passwords across the entire organization. DGN continues to use multi-factor authentication for all logins to DGN workstations. DGN reported the incident to Federal law enforcement. DGN also partnered with computer forensics professionals to thoroughly investigate the incident, notified potentially affected individuals about it, and implemented additional security solutions. DGN continues to evaluate ways to strengthen the security of its network going forward. DGN is also notifying other state regulators as necessary.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

**FREEMAN MATHIS & GARY, LLP**

/s/ *Nicholas Jajko*

Nicholas Jajko

# Exhibit “A”

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

DENNIS, GARTLAND & NIERGARTH
*Business Advisors Since 1973*

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

June 1, 2022

**Re: Notice of Data Security Incident**

Dear <<First Name>> <<Last Name>>,

We at DGN, LLC d/b/a Dennis, Gartland & Niergarth ("DGN") write to notify you of an incident that may affect the security of your personal information. This data was shared with DGN in the performance of services our firm provides to <<data owner>>. Please read this letter carefully.

***What Happened?***
On March 14, 2022, we learned that our organization was the victim of a computer malware incident. Upon discovery, we immediately shut down our network and commenced an investigation that included partnering with cyber security incident specialists to secure and fully restore our systems safely. We reported the incident to the IRS and Federal law enforcement. We determined that certain client files were obtained from our systems by someone outside the DGN organization. However, we cannot confirm with certainty when the access began or the full extent of which files were viewed or obtained by the unauthorized person. We do know that some files within the affected systems contained individuals' personal information and it is possible the unauthorized person viewed or obtained that information. Therefore, we performed a review of our internal records that concluded on March 28, 2022. On or about April 29, 2022 we notified impacted organizations, and thereafter we received authorization to provide you with this notification.

***What Information Was Involved?***
You are receiving this letter because one or more files containing your personal information, including your name, address, and potentially other sensitive information such as a Social Security number, driver's license/state identification number, date of birth, direct deposit financial information, and/or a passport or other secondary form of identification, could have been accessible on our servers and therefore, viewed during the period of compromise. However, we reiterate that our investigation did not definitively confirm that this occurred, and we have no knowledge of any actual misuse of personal information as a result of this incident at this time. Nonetheless, we believe it is important to notify you about this potential compromise out of an abundance of caution.

***What We Are Doing***
We take this event and the security of personal information entrusted to us very seriously and have taken steps to help mitigate the potential for harm and prevent this from happening again. After discovering the incident, we reset account and system passwords across the entire organization. We continue to use multi-factor authentication for all logins to DGN workstations. We reported the incident to Federal law enforcement. We also partnered with computer forensic professionals to thoroughly investigate the incident, notified potentially affected individuals about it, and implemented additional security solutions. We will also continue to evaluate ways to strengthen the security of our network going forward.

***What You Can Do***
We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or issuing bank immediately. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, should you find it appropriate to do so.

As an added precaution to help protect your identity, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Standard Time. Please note the deadline to enroll is July 28, 2022. You will find detailed instructions for enrollment on the enclosed Additional Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Again, at this time, there is no evidence that information has been misused as a result of this incident. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

***For More Information***
If you have any other questions or concerns, you may contact us at 1-800-939-4170 or go to https://app.idx.us/account-creation/protect for further information and assistance. We are very sorry for any concern or inconvenience this incident has caused or may cause you, and we encourage you to take advantage of the resources we are offering you. DGN remains committed to safeguarding the information in our care.

Sincerely,

Shelly Bedford

Shelly Bedford, CPA, MST, CVA
Managing Partner
DGN, LLC d/b/a Dennis, Gartland & Niergarth

## ADDITIONAL STEPS TO HELP PROTECT PERSONAL INFORMATION

**Take Advantage of the Services Offered to You.**

**1**. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. 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. 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.

**3. Telephone.** Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports which can be requested from each of the three major credit reporting companies (contact information below).

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

**Review personal account statements and credit reports.** We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

| Equifax | Experian | TransUnion |
|---|---|---|
| 1-888-298-0045 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |

**Report suspected fraud.** You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

**Place a Fraud Alert.** Consumers have the right to place a fraud alert on their credit file at no cost. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts are for one year and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide consumer reporting agencies by phone or online using the above contact information. For more information about placing a fraud alert, please visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

**Place a Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also

can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide consumer reporting agencies by phone or online using the contact information above. If you request a freeze online or by phone, the agency must place the freeze within one business day. For more information, about placing a security freeze, please visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

**Prevent Tax Fraud**. If you (or we) become aware of a fraudulent tax return filed in your name or you are instructed to do so by the IRS, you will need to work with your tax preparer to file the IRS Form 14039, Identity Theft Affidavit, with a paper copy of the return, and mail according to the instructions. A copy of this form can be found at https://www.irs.gov/pub/irs-pdf/f14039.pdf or https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. You may also visit https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft to contact the IRS's Identity Protection Specialized Unit (IPSU) at 800-908-4490. IPSU employees are available to answer questions about identity theft and resolve any tax account issues that resulted from identity theft. **NOTE**: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

**Obtain additional information** about the steps you can take to avoid identity theft from the following entities:

- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division may be contacted at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.oag.state.md.us/Consumer, and toll-free at (888) 743-0023 or (410) 528-8662.
- **All U.S. Residents:** The Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, and 1-877-IDTHEFT (438-4338).