GOODWIN

June 27, 2023

**VIA PORTAL**
**Maine Office of the Attorney General**
**6 State House Station**
**Augusta, ME 04333**

**Re: Notice Pursuant to Maine Revised Statutes 10 M.R.S.A. §§1346-1350-B**

Dear Attorney General Frey,

Pursuant to Maine Revised Statutes 10 M.R.S.A. sections 1346-1350-B, we write on behalf of Precision Imaging ("Precision" or "Company") to notify you of a data security matter, which we believe impacted approximately 4 Maine residents. Precision is a medical imaging center with four locations across the state of Florida.

Precision was the victim of a cybersecurity event that disrupted its service operations. Upon detecting suspicious activity on or around November 2, 2023, Precision promptly took steps to secure its network, including shutting down its systems, and initiating a comprehensive investigation into the matter with the assistance of third-party forensic specialists. As part of the investigation, the Company identified that files containing personal information were obtained by an unauthorized party. The Company then conducted a comprehensive evaluation of the potentially impacted data in order to determine the nature of personal information that may have been involved and the scope of the impacted population and to confirm address information for potentially impacted individuals. This process was completed on or around June 20, 2023.

Based on our investigation, the impacted population may have included 4 Maine residents. The types of personal information impacted will depend on the information the individual provided to Precision, but may include: first and last name; address; Social Security number; driver's license or government-issued identification number; health insurance information, medical condition(s) and diagnoses, or other health- or medical-related information; and dates of birth.

Notification of this matter was mailed to the impacted residents on or around June 22, 2023 A copy of this notification is attached as **Exhibit A**.

We currently have no evidence of misuse of any personal information as a result of this incident. In addition, we consulted with federal law enforcement throughout our investigation. Shortly after the cybersecurity event against Precision, federal law enforcement publicly reported that it had disrupted the operations of the high-profile threat actor group attributed to this incident, including through seizure of the group's servers and websites. We believe that such law enforcement disruption further mitigated additional risks to the impacted information. We continue to communicate and cooperate with law enforcement as part of the Company's efforts to address this matter and further protect patient information.

Precision takes the protection of patient information seriously. Precision is offering two years of identity protection services, at no cost, to affected patients through IDX. In addition, in response to this matter, Precision implemented measures to contain and remediate the incident and has taken steps to further secure the environment and enhance its security protocols, including by implementing new systems. The Company is also in the process of evaluating this matter further in order to prevent a similar occurrence in the future.

Below is the contact information for Joshua Hammond, CEO at Precision:

Joshua Hammond | CEO
Precision Imaging Centers
jhammond@precisioncenters.com

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

Kaylee Cox Bankston

# Exhibit A

PRECISION

Return to IDX
PO Box 480149
Niles, IL 60714

To Enroll, Please Call:
1-888-220-5769
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [XXXXXXXX]

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

June 22, 2023

**RE: NOTICE OF DATA BREACH**

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

We are contacting you regarding an incident at Precision Imaging ("Precision") that may have impacted some of your personal information. We are providing you with information about the incident and steps you may take to help protect your information.

**What Happened**

Precision was the victim of a cybersecurity event that disrupted its service operations. Upon detecting suspicious activity on or around November 2, 2022, Precision promptly took steps to secure our network, including shutting down our systems, and initiated a comprehensive investigation into the matter with the assistance of third-party forensic specialists. As part of the investigation, we identified that files containing personal information were obtained by an unauthorized party. We then conducted a comprehensive evaluation of the potentially impacted data in order to determine the nature of personal information that may have been involved and the scope of the impacted population and to confirm address information for potentially impacted individuals. This process was completed on or around June 20, 2023. Based on our comprehensive review, we determined that the impacted files may have included your personal information.

While we currently have no evidence of identity theft, fraud or other misuse of your information as a result of this matter, we are notifying you to provide you with information and steps you can take to help protect your information.

**What Information Was Involved**

The types of information that may have been impacted will depend on the information you have provided to Precision, but may include: first and last name; address; Social Security number; driver's license or government-issued identification number; health insurance information, medical condition(s) and diagnoses, or other health- or medical-related information; and dates of birth. ***At this time, we have no evidence of misuse of your personal information as a result of this incident.***

**What We Are Doing**

We take the protection of your information very seriously, and we sincerely regret that this incident occurred. To help further protect your information, we are providing you with **free identity protection services for 24 months,** as described in detail in this letter. Upon learning of this incident, we promptly initiated a comprehensive investigation to determine what occurred and retained third-party experts to assist with our investigation. We also implemented measures

to contain and remediate the incident and to further secure the environment, including by implementing new systems. We have also consulted with federal law enforcement in support of our investigation and response to this matter. In addition, we have taken steps to further enhance our security controls, including updates to processes and procedures, in an effort to prevent a similar occurrence from happening again.

**What You Can Do**

There are steps you can take to protect yourself in this situation, including enrolling in the identity protection service we are offering to you for free. Details regarding the service and how to enroll are provided below. As a best practice, we encourage you to remain vigilant for suspicious activity and to regularly review your financial statements and credit reports. We have also enclosed an attachment with additional information and resources where you can obtain additional information about identity theft and ways to protect yourself.

**What You Can Do**

We encourage you to contact IDX, A ZeroFox Company, the data breach and recovery services expert, with any questions and to enroll in the free identity protection services by calling 1-888-220-5769 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 Time. Please note the deadline to enroll is September 22, 2023.

Again, at this time, there is no evidence that your information has been misused; however, we encourage you to take full advantage of this service offering. IDX representatives can answer questions or concerns you may have regarding these services and the protection of your information.

**For More Information**

You will find detailed instructions for enrollment in the enclosed Additional Resources 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.

Please call 1-888-220-5769 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Joshua Hammond, CEO
Precision Imaging Center

## ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

**The Federal Trade Commission**

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

**Credit Reporting Agencies**

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| PO Box 740241 | PO Box 4500 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19016 |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

**Order Your Free Annual Credit Report.** You can order your free annual credit report online at www.annualcreditregort.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any 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 agency.

**Review Your Accounts and Report Unauthorized Activity.** We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

**Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

**Consider Placing a Security Freeze on Your Credit File.** You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

**Remain Vigilant and Lookout for Phishing Schemes.** We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing

schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

**For Maryland Residents:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General Consumer
Protection Division
200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

**For Massachusetts Residents:** You have the right to obtain a police report and to request a security freeze as described above. The credit reporting agencies may require certain personal information (e.g., name, Social Security number, date of birth, address) and valid identification (e.g., government-issued ID and proof of address, paystub, or statement) in order to implement your request for a security freeze. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

**For New York Residents:** You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office:

New York Attorney General's Office
Bureau of Consumer Frauds & Protection
The Capitol, Albany, NY 12224
1-800-771-7755
www.ag.ny.gov

**For North Carolina Residents:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center Raleigh,
NC 27699-9001
1-877-5-NO-SCAM
www.ncdoi.gov

**For Rhode Island Residents:** You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street Providence, RI 02903
1-401-274-4400
riag.ri.gov