

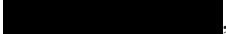


Return Mail Processing  
PO Box 509  
Claysburg PA 16625

December 17, 2024



Re: Notice of Data Security Incident

Dear ,

We are writing to notify you of the potential exposure of your personal information in a recent data security incident at Praedicat. There is no indication that your personal information was misused in any way that could cause harm to you, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation. Please read this letter carefully, because it provides details about what happened and what we are doing about it.

### **What Happened?**

As you may know, on November 26, 2024, Praedicat learned that data from its systems had been exfiltrated. Upon initial detection of the unauthorized activity, we immediately took containment steps and commenced an investigation. On December 4, 2024, Praedicat confirmed that certain files containing information related to your employment at Praedicat were impacted, such that your personal information may have been involved.

### **What Information Was Involved?**

The impacted information potentially included elements of your personnel file, including address, date of birth, last four digits of your Social Security number, insurance information, and/or passport or driver's license information, but only if you submitted such information to Praedicat Human Resources. There is no evidence that any of this information has been or will be publicly disclosed, or that any information was or will be misused for fraudulent purposes as a result of this incident, but we are communicating this to you so that you can take the steps outlined below to protect yourself.

### **What We Are Doing**

Immediately upon learning of this incident, we launched an investigation with the assistance of cybersecurity experts and outside lawyers, and in cooperation with law enforcement. Please be assured that we are working with experts to reinforce our systems and information security protocols in an effort to prevent incidents like this from occurring in the future.

We are also making resources available to those individuals whose information was involved. While we have no reason to believe that your information was used for any fraudulent purpose as a result of this incident, to help protect your identity, we are providing you with access to Experian IdentityWorks<sup>SM</sup> credit monitoring and

0000001



remediation services for 24 months at no charge to you. These services provide you with alerts for two years from the date of enrollment when changes occur to your credit file. These services also provide you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud.

### **How do I enroll for the free services?**

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection and credit monitoring tools available through Experian IdentityWorks. To enroll in these services at no charge, visit <https://www.experianidworks.com/credit> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll by March 31, 2025. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Should you have any questions regarding the Credit Monitoring services, have difficulty enrolling, or require additional support, please contact Experian at [REDACTED]. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

### **What You Can Do**

To help protect your personal information, we strongly recommend you take the following steps, all of which are good ideas in any event:

- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and restoration assistance if you were not the one who initiated it.
- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

### **For More Information**

If you have questions or concerns not answered by this letter, please contact Lisa Gallagher at (424) [REDACTED]. Please know that we take this matter very seriously, and we apologize for any concern this may cause.

Sincerely,



Dr. Robert T. Reville  
Chief Executive Officer  
Praedicat, Inc.

## **REFERENCE GUIDE**

If you suspect that you are a victim of identity theft or credit fraud, we encourage you to remain vigilant and consider taking the following steps:

**Order Your Free Credit Report.** To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the FTC's website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible if there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer credit reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumerfinance.gov> or [www.ftc.gov](http://www.ftc.gov).

**Place a Fraud Alert on Your Credit File:** A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below.

**Equifax**

[www.equifax.com](http://www.equifax.com)

1-800-525-6285

P.O. Box 740241

Atlanta, Georgia 30374-0241

**Experian**

[www.experian.com](http://www.experian.com)

1-888-397-3742

P.O. Box 9532

Allen, Texas 75013

**TransUnion**

[www.transunion.com](http://www.transunion.com)

1-800-680-7289

Fraud Victim Assistance

Division

P.O. Box 2000

Chester, Pennsylvania 19016

**Place a Security Freeze on Your Credit File.** You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus using the same contact information noted above.

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide: (1) Your full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security number; (3) Date of birth; (4) If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years; (5) Proof of current address, such as a current utility bill or telephone bill; (6) A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and (7) If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

**Contact the U.S. Federal Trade Commission.** If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.



- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338); [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**For Massachusetts Residents:** You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

**For New York Residents:** You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office  
Bureau of Internet and Technology  
(212) 416-8433  
<https://ag.ny.gov>

NYS Department of State's Division of Consumer  
Protection  
(800) 697-1220  
<https://www.dos.ny.gov/consumerprotection>

**For North Carolina Residents:** You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov).