



2000 Market Street
20th Floor
Philadelphia, PA 19103-3222
Tel 215.299.2000 Fax 215.299.2150
www.foxrothschild.com

CARLY E. NIXON
Direct No: 215.299.2845
Email: CNixon@FoxRothschild.com

May 24, 2023

Via email

Re: Notice of Data Breach

To Whom It May Concern:

Our office represents Precision Fabrics Group, Inc. ("Precision Fabrics"), and we are writing to provide you with notice of an event that may affect the personal information of two (2) Maryland residents. By providing this notice, Precision Fabrics does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction. Precision Fabrics may be supplemented with any material facts learned subsequent to its submission.

Background

On February 10, 2023, Precision Fabrics Group, Inc. ("Precision Fabrics") was a victim of a ransomware attack. Once the attack was discovered, Precision Fabrics engaged cybersecurity experts and launched an investigation into the nature and scope of the attack. As a result of the attack, the cybercriminals encrypted a Precision Fabrics system that stored information on current and former employees and their dependents. Precision Fabrics refused to pay the ransom to the cybercriminals. Between the initial attack to the mailing, Precision Fabrics worked to rebuild the impacted system, determine the notice population, and engaged notification vendors. Although there is no confirmation personal information was accessed or acquired as a result of the attack, personal information did reside on the encrypted system. Precision Fabrics is providing notice to individuals out of an abundance of caution. On This personal information included name and Social Security number. To date, there has been no indication of any misuse of the potentially impacted personal information.

Notice to Residents

A Pennsylvania Limited Liability Partnership

California Nevada Colorado New Jersey Delaware New York District of Columbia North Carolina Florida Oklahoma Georgia **Pennsylvania** Illinois South Carolina Massachusetts Texas Minnesota Washington Missouri

May 24, 2023

Page 2

Out of an abundance of caution, Precision Fabrics mailed written notice of this incident to potentially impacted individuals on May 24, 2023, in substantially the same form as the letter enclosed as Exhibit A.

Steps Taken

Precision Fabrics is offering impacted individuals with one (1) year of complimentary credit monitoring and identity restoration services, as well as additional information on how to protect against identity theft and fraud. In order to better protect against a similar incident from occurring in the future, Precision Fabrics is reviewing its policies and procedures, implementing Multi-Factor Authentication (MFA) on all accounts, and working with cybersecurity experts to implement additional safeguards to better protect against future incidents of this nature. In addition to providing this notice to your office, Precision Fabrics has provided notice of this incident to other state regulators and the consumer reporting agencies as required.

Contact

Should you have any questions regarding this notification or other aspects of this event, please contact me at cnixon@foxrothschild.com or 215-299-2845.

Sincerely,

Carly E. Nixon

Exhibit A



Return to IDX:
4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

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

<<First Name>> <<Last Name>>
<<Address>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

May 24, 2023

Re: Notice of Data Breach

Dear <<First Name>> <<Last Name>>:

I am writing to notify you of a recent incident that may impact your personal information. You are receiving this letter as a current or former employee of Precision Fabrics Group, Inc. ("Precision Fabrics").

What Happened? On February 10, 2023, Precision Fabrics was the victim of a ransomware attack. Once we discovered this, we immediately launched an investigation with the assistance of cybersecurity experts into the nature and scope of the attack. As part of the investigation, we have determined the perpetrators did obtain access to certain Company electronic data as a result of the ransomware. We have been able to mitigate the ransomware attack, but we do believe the perpetrators accessed certain systems that included limited information about current and former employees.

What Information Was Involved? The forensic investigation is concluded, and it has determined the perpetrators had access to systems storing names and Social Security numbers of current and former employees. At this time, we do not have any evidence that any of your personal information has been identified or discovered by the perpetrators, much less misused. As a precautionary measure, though, we are providing you with this notice.

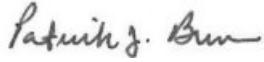
What Are We Doing? We take this incident and the security of your information seriously. In addition to taking the steps detailed above and providing this notice to you, we are reviewing our policies and procedures, implementing additional safeguards, and working with cybersecurity experts to better protect against an incident like this from happening again in the future. We are also offering you 1 year of complimentary credit monitoring and identity protection services with IDX, A ZeroFox Company. We have also notified the Federal Bureau of Investigation, and certain state regulators.

What You Can Do. You can review the enclosed **Steps You Can Take To Protect Your Information**, which contains instructions on how to enroll in the complimentary credit monitoring and identity protection services, as well as includes additional information on what you can do to better protect against the possibility of identity theft and fraud, if you feel it is appropriate to do so. Please note that while we will cover the cost of the identity protection services, you will need to complete the enrollment process.

For More Information. We understand you may have questions that are not answered in this letter. To ensure your questions are answered, please contact our dedicated call center at 1-800-939-4170. The call center is available Monday through Friday, between 9:00am and 9:00pm Eastern Time. Please note the deadline to enroll is August 24, 2023.

We sincerely regret any inconvenience or concern this event has caused you.

Very Truly Yours,

A handwritten signature in dark ink, appearing to read "Patrick J. Burns". The signature is fluid and cursive, with a long horizontal stroke at the end.

Patrick J. Burns
Chief Executive Officer
Precision Fabrics Group, Inc.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

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. 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 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 our 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.

You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069

www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013

www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000

www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.