

---

**Stephan Pelletier & Sons, Inc.**

56 Irving Rd  
Arundel, ME 04046  
207-294-2934  
brad@pelletierdrywall.com

27th September 2022

### INITIAL NOTIFICATION

Dear Employee,

Stephan Pelletier & Sons, Inc. (SPSI) is writing to make you aware of an incident that may affect the security of some of your information. We take this incident seriously and write to provide you with information about the incident, what we are doing in response, and the resources that are available to you to help better protect your information, should you feel it is appropriate to do so.

**What Happened?** On September 23, 2022, SPSI experienced unauthorized access to a business laptop.

**What Information Was Involved?** A comprehensive review of the involved systems was completed on September 24, 2022 and determined that the impacted files included information pertaining to certain current and former SPSI employees. We are notifying you now because our investigation identified that your name, social security number, and bank routing and account numbers associated with your payroll direct deposit were present at the time of this activity. SPSI is not aware of any actual or attempted misuse of this information and is notifying you out of an abundance of caution.

**What We Are Doing.** We take this incident and the security of information within our care seriously. We are notifying potentially affected individuals, including you, so that you may take further steps to protect your information, should you feel it is appropriate to do so. As an added precaution, we are working on providing identity theft protection for one year at no cost to you. Additional information will be provided as it becomes available via written notification.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. As communicated via telephone on September 24, 2022- we recommend contacting your financial institution where you receive your direct deposit to

---

alert them of this potential data breach so they may offer additional steps to take regarding their practices. This letter also provides other precautionary measures you can take to help protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. You may also enroll in the complimentary identity theft protection services we will be making available to you.

Please accept our apologies that this incident occurred. We understand you may have additional questions not addressed by this letter. If you have questions, please contact us at 207-294-2934 during the hours of 9 AM and 5 PM.

Sincerely,

Stephan Pelletier & Sons, Inc.

**– OTHER IMPORTANT INFORMATION –**

**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 one (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 105069 Atlanta, GA 30348*

*<https://www.equifax.com/personal/creditreport-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/fraudalerts>  
(800) 680-7289*

**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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

---

*Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348*  
*<https://www.equifax.com/personal/creditreport-services/credit-freeze/>*  
*(888) 298-0045*

*Experian Security Freeze P.O. Box 9554 Allen, TX 75013*  
*<http://experian.com/freeze>*  
*(888) 397-3742*

*TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094*  
*<https://www.transunion.com/creditfreeze>*  
*(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 reporting 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.

### **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](http://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.

### **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](http://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 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.