Template Message to Current or Prior Employees/Job Applicants whose files may have been accessed:

Subject: **Notice of February 5, 2022 Data Security Incident, New or Extended Protective Measures Against Identity/Credit Theft**

Notice of February 5, Data Security Incident:

As current employees may be aware, on February 5, 2022 Portland Airfreight Inc. (PAF) again experienced an unauthorized system lockdown to our computer system (the February 5, 2022 Incident), which was similar in many respect to a prior incident on December 2, 2021 (the December 2, 2021 Incident), which was the subject of our earlier notice to you.

As with the December 2, 2021 Incident, we immediately engaged computer forensic services, and must acknowledge the potential that personally identifiable information (PII) from our personnel files and potentially other information from our computer system may have been accessed and/or copied or was otherwise stolen as a result of unauthorized access to our system beginning in the early morning hours of February 5, 2021.

We understand that the PII potentially accessed or taken may include Social Security numbers (SSNs), drivers' license numbers, birthdates, and telephone and address information from such files among other information resident on our system.

As a result of the investigation, we have been advised that the system lock out resulted from the installation of ransomware known as "KTC Ransomware,"

Since the access to PAF's system may have been widespread and could have included email and other files where PII may be, you should consider whether information which you maintained could have included additional PII whose compromise must be addressed.

PAF has not attempted to contact the criminals responsible for this February 5, 2022 attack on our computer system, and has not been contacted by them. PAF has no plans to pay ransom. PAF has notified the FBI and state attorneys general here and in Maine. We have also solicited and will implement all reasonable additional security measures in connection with our computer system, and will be considering additional measures and policies to strengthen our system and reduce this risk which faces PAF and everyone who uses computer systems and the internet.

What You Can Do To Minimize Your Risks Of And Mitigate The Impacts Of Identity Theft

The principal risks from stolen PII include unauthorized credit risks and risks to governmental transactions including tax returns and government benefits. Attached to this email is a pdf from the IRS reflecting governmental resources.

With respect to risks involving tax refunds and social security benefits, we include a copy of a detailed IRS pamphlet as an attachment to this email which includes further specific links for reporting and monitoring.

With respect to unauthorized credit risks, it is recommended that you immediately lock down your credit reports with each of the credit rating agencies (E.g. Transunion, Experian, etc.) if you have not already done so. When locked, no third parties are allowed to make credit inquiries even if they have your social security number, unless and until you unlock your account for that purpose. Further

information on this process is available here: https://www.nerdwallet.com/article/finance/how-to-freeze-credit

While some commentators believe that third party credit and/or identity theft monitoring is unnecessary if your credit reports are locked, we leave that decision to you and are willing to reimburse the reasonable costs of such monitoring for a period of 3 months for any employee, with copies of the monitoring reporting from the service. For example, we note that Equifax Complete provides such services for 19.95 per month. Other similar reasonable cost services may be used with our prior consent.