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

Subject: Notice of Data Breach, Protective Measures Against Identity/Credit Theft

Notice of Breach Incident:

As you may be aware, beginning on December 3, 2021 we experienced an unauthorized system lockdown to our computer system. We immediately engaged computer forensic services, and have very recently learned that there is a significant likelihood that personally identifiable information (PII) from our personnel files and potentially other information from our computer system have been accessed and likely copied or otherwise stolen as a result of unauthorized access to our system beginning in the evening of December 2, 2021.

We understand that the PII 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.

We immediately retained computer forensic consultants who began their investigation the following Monday. As a result of the investigation, we were very recently advised that the system lock out resulted from the installation of ransomware known as "Lockbit 2.0" and the types of files (personnel files) which were accessed and likely copied in addition to the installed ransomware message.

Since the access to our system was 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.

We have not attempted to contact the criminals responsible for this attack on our computer system but we have notified the FBI and state attorneys general here and in Maine. We have also implemented 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 And 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.

Securing today and tomorrow

Identity Theft and Your Social Security Number

SSA.gov

Identity theft is one of the fastest growing crimes in America. A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.

Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

Your number is confidential

The Social Security Administration protects your Social Security number and keeps your records confidential. We don't give your number to anyone, except when authorized by law. You should be careful about sharing your number, even when you're asked for it. You should ask why your number is needed, how it'll be used, and what will happen if you refuse. The answers to these questions can help you decide if you want to give out your Social Security number.

How might someone steal your number?

Identity thieves get your personal information by:

- Stealing wallets, purses, and your mail (bank and credit card statements, pre-approved credit offers, new checks, and tax information).
- Stealing personal information you provide to an unsecured site online, from business or personnel records at work, and personal information in your home.
- Rummaging through your trash, the trash of businesses, and public trash dumps for personal data.
- Buying personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit.
- Posing by phone or email as someone who legitimately needs information about you, such as employers, landlords, or government agencies.

Be careful with your Social Security card and number

When you start a job, make sure your employer has your correct Social Security number so your records are correct. Provide your Social Security number to your financial institution(s) for

tax reporting purposes. Keep your card and any other document that shows your Social Security number in a safe place. DO NOT routinely carry your card or other documents that display your number.

What if you think someone is using your number?

Sometimes more than one person uses the same Social Security number, either on purpose or by accident. If you suspect someone is using your number for work purposes, you should contact us to report the problem. We'll review your earnings with you to ensure our records are correct.

You also may review earnings posted to your record on your *Social Security Statement*. The *Statement* is available online to workers age 18 and older. To get your *Statement*, go to ***www.ssa.gov/myaccount*** and create an account.

What if an identity thief is creating credit problems for you?

If someone has misused your Social Security number or other personal information to create credit or other problems for you, Social Security can't resolve these problems. But there are several things you should do.

Visit ***IdentityTheft.gov*** to report identity theft and get a recovery plan. ***IdentityTheft.gov*** guides you through each step of the recovery process. It's a one-stop resource managed by the Federal Trade Commission, the nation's consumer protection agency. You can also call **1-877-IDTHEFT** (**1-877-438-4338**); TTY **1-866-653-4261**.

You may want to contact the Internal Revenue Service (IRS). An identity thief also might use your Social Security number to file a tax return to receive your refund. If you're eligible for a refund, a thief could file a tax return before you do and get your refund. Then, when you do file, the IRS will think you already received your refund. If your Social Security number is stolen, another person may use it to get a job. That person's employer would report earned income to the IRS using your Social Security number. This will make it appear that you didn't report all of your income on your tax return. If you think you may have tax issues because someone has stolen your identity, go to ***www.irs.gov/uac/Identity-Protection*** or call **1-800-908-4490**.

Also, you should file an online complaint with the Internet Crime Complaint Center (IC3) at ***www.ic3.gov***.

The IC3 gives victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations.

IC3 sends every complaint to one or more law enforcement or regulatory agencies with jurisdiction.

IC3's mission is to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The IC3 serves the broader law enforcement community that combats internet crime. This includes federal, state, local, and international agencies.

The IC3 reflects a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance.

You should also monitor your credit report periodically. You can get free credit reports online at ***www.annualcreditreport.com***.

Should you get a new Social Security number?

If you've done all you can to fix the problems resulting from misuse of your Social Security number, and someone is still using your number, we may assign you a new number.

You can't get a new Social Security number:

- If your Social Security card is lost or stolen, but there's no evidence that someone is using your number.
- To avoid the consequences of filing for bankruptcy.

- If you intend to avoid the law or any legal responsibility.

If you decide to apply for a new number, you'll need to prove your identity, age, and U.S. citizenship or immigration status. For more information, ask for *Your Social Security Number and Card* (Publication Number 05-10002). You'll also need to provide evidence that you're having ongoing problems because of the misuse.

Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

If you receive a new Social Security number, you shouldn't use the old number anymore.

For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.

Contacting Social Security

The most convenient way to do business with us from anywhere, on any device, is to visit ***www.ssa.gov***. There are several things you can do online: apply for benefits; get useful information; find publications; and get answers to frequently asked questions.

Or, you can call us toll-free at **1-800-772-1213** or at **1-800-325-0778** (TTY) if you're deaf or hard of hearing. We can answer your call from 7 a.m. to 7 p.m., weekdays. You can also use our automated services via telephone, 24 hours a day. We look forward to serving you.

Social Security Administration
Publication No. 05-10064
July 2021 (June 2018 edition may be used)
Identity Theft and Your Social Security Number
Produced and published at U.S. taxpayer expense