Burning Man
660 Alabama St., 4th Fl
San Francisco. CA 94110

[Date]

[Recipient's Name]
[Address]
[City, State, Zip]

Re: Supplemental Notice of Data Breach

Dear [Name]:

At Burning Man Project ("Burning Man"), we value and respect the privacy of your information, which is why we are writing to supplement the email that we sent to you on December 3, 2023. As stated in the email, we learned that a Burning Man Project employee emailed certain individuals who were either eligible for or participated in a 401(k) plan during the course of their employment, and inadvertently included the wrong attachment. While we are not aware of any misuse of your information, we are providing this notice to update you on the incident and to call your attention to steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened?

On December 3, 2023, Burning Man discovered that one of its employees had inadvertently included a mislabeled document in an email with the subject line "Burning Man Project | Important: 401(k) Annual Participant Notices and Disclosures." The email was sent to 154 Burning Man current or former employees who presently participate in or became eligible for our 401(k) plan during the course of their employment. One of the documents attached to the email contained personal information for 227 current or former employees.

What Information Was Involved?

This incident involved the following types of data: names, dates of birth, home addresses, Social Security numbers, email addresses, date of hire, and 401(k) plan eligibility status.

What We Are Doing.

Burning Man takes this incident and the security of your personal information very seriously. Upon learning of this incident, we launched an in-depth investigation to determine the scope of the incident and identify those potentially affected. This included working with our information technology team in an effort to ensure the incident did not result in any additional exposure to personal information. We took steps to retract the email and/or request that email recipients delete both the email from their inbox and trash. Even if you did not receive the email sent on December 3, your personal information was included in the attachment. This communication was not delayed at the request of law enforcement. As an added precaution, we are also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services through Norton Lifelock. If you wish to receive these services, activation instructions are below.

What You Can Do.

The attached sheet describes steps you can take to protect your identity and personal information. To help protect your identity, we are offering complimentary access to Norton LifeLock through December 31, 2024. To activate your membership and start monitoring your personal information, please follow the steps below:

- The enrollment period begins December 8, 2023 and ends December 31, 2024. You can enroll any time during this period.
- To enroll, please fill out this short form at https://www.surveymonkey.com/r/BMP-LifeLock to consent to Burning Man Project setting up an account for you.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, please email privacysupport@burningman.org. In addition to taking advantage of the credit monitoring and identity restoration services outlined above, set forth in the attached guide are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s).

For More Information.

Burning Man apologizes for the inconvenience this may cause. We are committed to maintaining the security and privacy of personal information. We want you to be assured that we are taking steps to minimize the chances of a similar occurrence happening again. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, email us at our dedicated support email at privacysupport@burningman.org.

Regards,

Steven Blumenfeld
Chief Technology Officer
Burning Man Project

ADDITIONAL RECOMMENDED STEPS

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. 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 in the event 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 reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.

- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also 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 place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

  Equifax
  P.O. Box 105069
  Atlanta, GA 30374
  1-800-525-6285
  www.equifax.com

  Experian
  P.O. Box 9554
  Allen, TX 75013
  1-888-397-3742
  www.experian.com

  TransUnion
  P.O. Box 2000
  Chester, PA 19016
  1-800-680-7289
  www.transunion.com

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information

periodically since identity thieves sometimes hold on to stolen personal information before using it.

- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. 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/or the Federal Trade Commission ("FTC"). 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 at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

- *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: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.