20439

[AFF LETTERHEAD]

April 30, 2021

Via First Class Mail and Email
[insert name, address, email]

RE: Notice of Data Incident

Dear ____,

I am writing to inform on behalf of the American Forest Foundation (AFF) that over the past two months we have been investigating and monitoring a breach of a single employee email account. Our investigation focused on determining what type of information may have been accessed and to ensure that no wider organizational harm was caused. The first unauthorized login occurred on December 1, 2020. The incident turned out to be a failed attempt to engage in a wire transfer fraud on AFF. Through our investigation we have however identified a low risk of some personal employee data that could have been exposed during the incident. This data was included in password-protected email attachments and may include personal information about you, including your first name, last name, social security number, state tax withholding amounts, and other employment-related information. We have no reason to believe that the data included in these files was or is being misused. The compromised email account has been promptly reinstated and the incident resolved. In addition, out of an abundance of caution we are taking the following steps:

Emails originated from an external sender have been marked with the following message "CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders."

We will be reaching out to employees that have been flagged for further training through our proactive phishing vulnerability testing.

We are asking that all employees follow our protocols for email account password reset and multi factor verification carefully. If you did not initiate a sign in, do not approve a multi-factor challenge. Only text message verification codes can be used. Phone multi-factor verification is no longer an option.

We are now asking all employees to apply a high degree of caution on the content of files attached to emails. At no time should a file containing social security numbers or banking details of employees, partners, contractors, or landowners be shared by email. Teams regularly handling this type of information have already been notified of additional security protocols, but we are asking for your help in ensuring that this type of sensitive data is handled appropriately. Files with personal data should only be shared securely by providing a link to one of our internal file servers on Cabinets, Dropbox, or Sharepoint. If you need to request this type of file from an external party, please use a secure file transfer service. Contact Alastair Jarvis our VP of Entrepreneurship and Technology Strategy if you have any questions about how to do this.

Any US based employee will be offered credit monitoring services for the next 18 months. This is a voluntary service to protect you in the unlikely event that your personal information was accessed. If you would like to opt into this service, simply reply to this email directly or call [insert number] and we will work with you to set up your credit monitoring account.

I appreciate everyone's diligence in maintaining cyber security for our work. Despite our best efforts to apply security protocols, data breaches are a reality of the world we live in. Working together to manage digital information carefully can have a big influence on our ability to contain any potential damage to our shared interests.

Thank you for your care and attention in keeping our work safe. We are sending this notice via email and regular mail to ensure that you receive it.

Sincerely,

STEPS YOU CAN TAKE TO PREVENT IDENTIY THEFT AND FRAUD

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

To monitor for actual or attempted misuse of Social Security benefits, you can create an account at https://www.socialsecurity.gov/myaccount. If you see an error or attempted misuse of social security benefits, you can go to your local Social Security Office for assistance. Local offices can be found using the following office locator - https://secure.ssa.gov/ICON/main.jsp.

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. You have the right to file a police report. This notice has not been delayed by law enforcement.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Washington, DC residents: The Attorney General Can be contacted at 400 6th St NW, Washington, DC 20001 oag@dc.gov, (202) 727-3400, www.dc.gov