NOTICE OF DATA BREACH

April XX, 2016

Name
Address 1
Address 2
City, State Zip Code

Dear _____:

I am writing to provide you formal written notice of a possible data breach involving your IRS Form W-2. While our investigation is on-going, we believe that your W-2 form was likely improperly downloaded by an unauthorized person from our third-party service provider, Equifax. On behalf of Stanford University, please accept our sincere apology for any concerns that this incident may cause you.

What Happened

During the latter half of March 2016, a small number of employees reported to Stanford University's Department of Public Safety (DPS) and Information Security Office that they had been unable to file their tax returns because fraudulent returns had already been filed using their information. University officials began to investigate the matter immediately.

On April 4, 2016, University officials determined that Stanford University had been specifically targeted as a source of W-2 forms. Stanford University makes its W-2 forms available to current and former employees through W-2Express, which is an online service owned by the credit bureau, Equifax. Downloads from W-2Express require knowledge of an individual's Social Security Number and date of birth. At this time, we have no reason to believe that your Social Security Number and date of birth were obtained from Stanford systems. However, as stated above, your W-2 form was among those that were downloaded from Equifax. We do not have any information as to whether a tax return in your name has been filed fraudulently with the IRS or your state tax agency.

What Information Was Involved

The W-2 form included your:

- first name
- last name
- address
- date of birth
- Social Security Number
- wage information; and,
- tax information

As stated above, in order to download the W-2, an unauthorized person would have had to already have access to your Social Security number and birthdate.

What We Are Doing

The W-2Express service was disabled on April 5, 2016, promptly upon discovering the fraudulent access to the W-2 forms.

University officials are working closely with Equifax and law enforcement to investigate further and review our procedures in order to help to prevent this type of incident in the future.

On April 4, 2016, DPS and the Information Security Office issued an alert about tax fraud to the Stanford Community. Additionally, on April 7, 2016, the Vice President of Business Affairs and CFO emailed all Stanford employees to inform them of this matter and the University's investigation. This announcement was also included in the Stanford Report newsletter on April 8, 2016. University officials also issued an email communication to potentially affected individuals, for whom we had an email address, on April 14, 2016, and this email included information about enrolling in credit monitoring and protection services from Equifax.

In order to safeguard your personal information, we are providing you with two comparable credit monitoring and protection services options, AllClear Pro TBO™ and Equifax ID Patrol™. We encourage you to review both offerings and choose the one that is best for you. You may also enroll in both services at no charge to you.

AllClear Pro TBO™ includes both of the following services:

- AllClear SECURE: AllClear ID can provide you with identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, call 855-904-5737 and an investigator will help you recover your financial losses, restore your credit and return your identity to its proper condition.

- AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-904-5737 and using the following redemption code: {RedemptionCode}. This code is personal to you and should not be shared with others.

  Please note, additional steps may be required by you in order to activate your phone alerts and monitoring options.

Equifax ID Patrol™
Equifax will provide you with credit monitoring services, "ID Patrol", for 24 months. ID Patrol includes credit monitoring and $1 million of identity theft insurance coverage that provides reimbursement of certain costs related to recovering your identity. You can sign up online at www.myservices.equifax.com/patrol using the following unique activation code:{ActivationCode}. Please note that this information was provided to you in email communication dated April 14, 2016, and there are no additional actions required if you have already activated this service. This code is personal to you and should not be shared with others.

What You Can Do
If you have not already done so, we advise you to file your tax returns as you normally would.

If you believe that your W-2 form was downloaded by an unauthorized person, you should file IRS Form 14039 Identity Theft Affidavit with the IRS. The form is attached to this letter. The IRS has a Taxpayer Guide to Identity Theft, which we recommend you review here: https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. Part of that guide provides:

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- *Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.*
- *Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.*
- *Continue to pay your taxes and file your tax return, even if you must do so by paper.*

If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

We recommend that you enroll in one of the credit monitoring services being offered above and review the additional resources enclosed with this letter.

We encourage you to continue to take steps to help protect yourself from the fraudulent use of your identity. You should always remain vigilant and check your account statements regularly. Even if you do not find any signs of fraud on your credit reports, the California Privacy Enforcement and Protection Unit recommends that you check your credit reports every three months for the next year. The law allows you to order a free credit report from each of the three national credit reporting agencies every 12 months. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to monitor the accuracy and completeness of the information in your reports. To obtain your credit reports, visit annualcreditreport.com or call toll-free 1-877-322-8228. Note that this is the only website authorized by the federal government to fill orders for the free annual credit report. Beware of imposter websites that offer similar services.

You may also wish to contact the three major credit reporting agencies directly for any concerns or changes to your credit report. The agencies can be contacted as shown:

Equifax, Inc.
Equifax Credit Information Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
Toll-Free: 1-800-525-6285

Experian PLC
P.O. Box 9532
Allen, TX 75013
www.experian.com
Toll-Free: 1-888-397-3742

TransUnion, LLC
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19016
www.transunion.com
Toll-Free: 1-800-680-7289

Report any suspected identity theft to your local law enforcement and to the FTC.

For More Information

We encourage you to continue to take steps to help protect yourself from the fraudulent use of your identity. The Information Security Office provides specific guidance to the Stanford community on how to avoid, detect and handle identity theft at https://security.stanford.edu/identity-theft.

We want to assure you that Stanford University is committed to protecting the privacy of its current and former employees. If you have any questions or concerns or would like to talk to someone about this letter, you may contact Stanford's Financial Support Center at 650-723-2772 or email finhelp@stanford.edu.

Sincerely,

Randy Livingston
Vice President for Business Affairs
and Chief Financial Officer
Stanford University

IF YOU ARE A CALIFORNIA RESIDENT: For more information on identity theft, you may visit the California Office of Privacy Protection website, www.oag.ca.gov/privacy.

IF YOU ARE AN INDIANA RESIDENT: For additional steps you may want to take to protect yourself please read the Indiana Identity Theft Prevention section online at www.IndianaConsumer.com for more information about situation-specific actions and responses.

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
http://www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: For more information on identity theft, we suggest that you visit the New York State Consumer Protection Board website at www.dos.ny.gov/consumerprotection.

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
http://www.ncdoj.com