



December 20, 2017

NOTICE OF DATA BREACH

[Name]
[Address 1]
[Address 2]
[City, State zip]

Dear _____:

I am writing to provide you formal written notice of a possible data breach involving your personal information. We believe that personal information that you provided to the Graduate School of Business prior to traveling with the university between 1995 and 2002 was accessible to faculty, staff and students at the Graduate School of Business from 2000 through early December 2017. On behalf of Stanford University, please accept our sincere apology.

What Happened

On October 27, 2017, the University Privacy Office (“UPO”) received a report that several folders with confidential information on a shared file server maintained by the Graduate School of Business (“GSB”) were accessible to GSB faculty, staff and students. The GSB IT team became aware of the incorrect folder permissions on February 23, 2017, however, because GSB did not appreciate the scope of the exposure there was a delay in informing the UPO. Following notification, the UPO engaged a third-party forensics team and undertook a comprehensive review of all the files accessible to the GSB community, and last week discovered several folders maintained by student organizations with student personally identifiable information. The information was collected by certain student organizations from then students for a variety of purposes, including international travel, travel reimbursement and employment/internship applications. *We do not have any direct evidence that the file containing your personal information was actually accessed, downloaded or used by any unauthorized person.* However, out of an abundance of caution, we believe that it is important that we notify you so that you can take steps to protect yourself.

What Information Was Involved

The file included your:

- first name;
- last name;
- Social Security Number;
- passport number (if applicable)

What We Are Doing

The exposed files were removed from the shared environment upon identifying the files. The UPO verified that the current traveler Personal Information Form sits in a secured environment with limited accessibility.



The university engaged a data forensics firm to identify personally identifiable information in the accessible files and to validate file permissions at the time of the incident. This part of the investigation is on-going until we are assured that we have identified all personally identifiable information in the folders.

The university CIO Council will review and make recommendations for enhancing secure file sharing across the university.

What You Can Do

In order to safeguard your personal information, we are providing you with credit monitoring and credit repair services. If you are a current university employee, you may enroll by following the steps detailed here:

<https://cardinalatwork.stanford.edu/benefits-rewards/health/medical-life/voluntary-benefits/identity-theft-protection> or <https://goo.gl/Gc5Hgx>.

If you are no longer employed with Stanford University, credit monitoring services can be obtained by contacting ID Experts to enroll in free MyIDCare services. Please call [phone number] or go to <https://ide.myidcare.com/stanford> and use the Access Code provided above. MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note that the deadline to enroll is March 20, 2018

We recommend that you enroll in one of the credit monitoring services being offered above and monitor your credit report with one of the credit monitoring agencies listed in this letter. 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 www.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. We recommend that you proactively freeze your credit to block credit inquiries by contacting each of the three credit reporting agencies. The agencies can be contacted as shown below:

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

www.transunion.com
Toll-Free: 1-800-680-7289

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

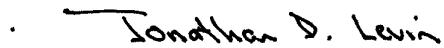
TransUnion, LLC
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19016

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 the dedicated call center at [number]. Again, we sincerely apologize for the potential exposure of your personally identifiable information.

Sincerely,

Jonathan D. Levin

Jonathan D. Levin
Dean, Graduate School of Business