



c/o ID Experts
P.O. Box 10444
Dublin, Oh 43017-4044

To Enroll, Please Call:
888-684-4998
Or Visit:
<https://ide.myidcare.com/stanford>
Enrollment Code: [XXXXXXXXXX]

[Name]
[Address1]
[Address2]
[City, State Zip]

December 1, 2017

Notice of Data Breach

Dear <First Name> <Last Name>,

I am writing to provide you formal written notice of a possible data breach involving your personal information. We believe that a report created in August 2008 containing your personal employee information was accessible to faculty, staff and students at the Graduate School of Business from mid-September 2016 through early March 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 permissions on these folders were incorrectly changed around September 2016, and thus the included files were viewable by the GSB community. The GSB IT team became aware of the incorrect folder permissions on February 23, 2017. They adequately locked down the impacted folders by March 3rd. However, because GSB did not appreciate the scope of the exposure there was a delay in informing the UPO. Following notification, the UPO undertook a comprehensive review of all the files accessible to the GSB community, and last week discovered a file with employee personal information. *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;
- date of birth;
- Social Security Number; and,
- annual benefits base salary

What We Are Doing

The exposed folders were secured within eight days of GSB IT learning of the issue. The Information Security Office independently verified that appropriate file permissions were set.

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 Information Security Office, in coordination with university IT leadership, 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 888-684-4998 or go to <https://ide.myidcare.com/stanford> and use the enrollment code provided at the top of this notice. MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note that the deadline to enroll is March 1, 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

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

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 888-684-4998. Again, we sincerely apologize for the potential exposure of your personally identifiable information.

Sincerely,



Randy Livingston
Vice President for Business Affairs