



mwe.com

David Saunders
Attorney at Law
dsaunders@mwe.com
+1 312 803 8305

February 16, 2023

VIA EMAIL AND US MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

I write on behalf of the Stanford University (“Stanford”), with respect to a data security event involving certain personal information of eleven Maryland residents. By providing this notice, Stanford does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Stanford’s Department of Economics maintains a folder containing .pdf copies of the applications of the Department’s 2022-23 PhD program applicants. Access to the contents of the folder is restricted to authorized users within the Department of Economics. Due to human error, the access permissions of the folder were changed from private to public on December 5, 2022. Therefore, access to the folder with .pdf copies of the applications was inadvertently available to anyone who clicked on the link. After a Stanford PhD student notified Stanford of the unrestricted access on January 24, 2023, Stanford immediately locked the folder from public access and limited access to authorized users.

Stanford immediately initiated an investigation of the incident and by reviewing access logs on January 27, 2023, Stanford identified three instances of unauthorized access (two instances of unauthorized downloads and one instance of unauthorized view) of files in the folder.

Since the end of January, Stanford has worked to individually review all applications, in order to identify the affected applicants, as well the nature of the data categories impacted and to determine the best measures to mitigate the risks for the affected applicants. That process proved to be time-consuming and did not complete until mid-February.

As part of this review, Stanford was able to identify the affected applicants, which included eleven Maryland residents. An application includes identification data (e.g. full name, date of birth, home and mailing addresses, phone number(s), email address, citizenship country/status), visa status (in order to ensure that applicants can enter the territory of the United States if accepted), and information supporting the application such as education and professional experiences (e.g., grades and transcripts from previous

**McDermott
Will & Emery**

444 West Lake Street Chicago IL 60606-0029 Tel +1 312 372 2000 Fax +1 312 984 7700

US practice conducted through McDermott Will & Emery LLP.

Office of the Attorney General
February 16, 2023
Page 2

educational institutions, résumé, personal essay(s), letters of recommendations and recommenders' evaluation of applicant).

Stanford has taken steps to enhance its data privacy and security measures to prevent the occurrence of a similar event in the future. A memo to all graduate admission officers at Stanford was sent from the Chief Information Security Officer requiring verification that all graduate applications within the department are protected and secured. In addition, Stanford will review its information security policies periodically and send emails regarding information security issues periodically to raise awareness of Stanford personnel to data privacy and security requirements.

Stanford will send a notification letter to the affected Maryland residents on February 17, 2023 via regular U.S. mail and email. A copy of the template notification letters are enclosed. In addition, Stanford is offering complimentary credit monitoring and identity protection services through IDX for 24 months to individuals whose Social Security Number was exposed, and all impacted individuals will be receiving 24 months of dark web monitoring through IDX.

If you have any questions, please contact me at dsaunders@mwe.com at 312-803-8305.

Sincerely,

A handwritten signature in blue ink, appearing to read 'D. Saunders', with a stylized flourish at the end.

David Saunders

Enclosures

**McDermott
Will & Emery**

Stanford University
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code:
<<XXXXXXXXXX>>

Stanford University

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

February 17, 2023

<<INFORMATION ABOUT A DATA INCIDENT/NOTICE OF DATA BREACH>>

Dear <<First Name>> <<Last Name>>,

I am writing to notify you of a recent data incident at Stanford University, which includes information you submitted for your graduate application to Stanford's Department of Economics. We would like to make sure you know the facts about what happened, what information was involved, the steps we are taking to help protect you, and how to reach us if you have any questions. As a result of this incident, we have partnered with IDX to provide you with this notification.

What Happened?

On January 24, 2023, Stanford was notified that a folder containing the 2022-23 application files for admission to Stanford's Department of Economics' Ph.D. program was available through the department's website because of a misconfiguration of the folder's settings. Once this was reported, access to the folder was immediately restricted. We promptly investigated this matter, which revealed that the unrestricted access to the applications began on December 5, 2022, and that there were two downloads of the application materials between December 5, 2022, and January 24, 2023. We do not have evidence that the information has been misused.

What Information Was Involved?

The information involved in this incident includes your application and accompanying materials. Personal data in the application includes your first and last name, date of birth, home and mailing addresses, phone number, email address, race and ethnicity, citizenship, and gender. <<Impacted Data >> Also, your submitted materials include your transcript(s), personal statements, résumé, and letters of recommendation.

(<<Please note that no Stanford evaluative content{, U.S. Social Security Number} or financial data was contained in your application file.>>)

What We Are Doing

The confidentiality, privacy, and security of personal information are among our highest priorities, and we have security measures in place to protect this type of information. In response to this incident, we are updating our processes and policies related to electronic file storage security and will be retraining faculty and staff on the policies.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling this toll free number 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided at the top of this letter. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 16, 2023.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

If you have any questions or concerns, please contact IDX at their toll free number: 1-800-939-4170.

We sincerely regret any inconvenience this incident may cause you.

Sincerely,



Raina Rose Tagle

Senior Associate Vice President and Chief Risk Officer

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Restoration

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Iowa residents, State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Pro-Tem, Inc. dba PTI Systems is located at 2525 South Shore Boulevard, Suite 401 League City, TX 77573.

For Massachusetts residents, You have the right to obtain a police report if you are the victim of identity theft.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

Stanford University
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

Stanford University

To Enroll, Please Call:

1-800-939-4170

Or Visit:

[https://app.idx.us/account-](https://app.idx.us/account-creation/protect)

[creation/protect](https://app.idx.us/account-creation/protect)

Enrollment Code:

<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

February 17, 2023

<<INFORMATION ABOUT A DATA INCIDENT/NOTICE OF DATA BREACH>>

Dear <<First Name>> <<Last Name>>,

I am writing to notify you of a recent data incident at Stanford University, which includes information you submitted for your graduate application to Stanford's Department of Economics. We would like to make sure you know the facts about what happened, what information was involved, the steps we are taking to help protect you, and how to reach us if you have any questions. As a result of this incident, we have partnered with IDX to provide you with this notification.

What Happened?

On January 24, 2023, Stanford was notified that a folder containing the 2022-23 application files for admission to Stanford's Department of Economics' Ph.D. program was available through the department's website because of a misconfiguration of the folder's settings. Once this was reported, access to the folder was immediately restricted. We promptly investigated this matter, which revealed that the unrestricted access to the applications began on December 5, 2022, and that there were two downloads of the application materials between December 5, 2022, and January 24, 2023. We do not have evidence that the information has been misused.

What Information Was Involved?

The information involved in this incident includes your application and accompanying materials. Personal data in the application includes your first and last name, date of birth, home and mailing addresses, phone number, email address, race and ethnicity, citizenship, and gender. Also, your submitted materials include your transcript(s), personal statements, résumé, and letters of recommendation. <<As a reminder, your submitted materials included health information about you.>>

(Please note that no Stanford evaluative content, U.S. Social Security Number or financial data was contained in your application file.)

What We Are Doing

The confidentiality, privacy, and security of personal information are among our highest priorities, and we have security measures in place to protect this type of information. In response to this incident, we are updating our processes and policies related to electronic file storage security and will be retraining faculty and staff on the policies.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of CyberScan and Social Media monitoring, and Password Detective.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling this toll free number 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided at the top of this letter. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 17, 2023.

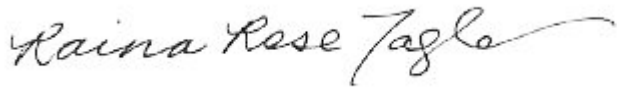
Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

If you have any questions or concerns, please contact IDX at their toll free number: 1-800-939-4170.

We sincerely regret any inconvenience this incident may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Raina Rose Tagle". The signature is written in dark ink and has a fluid, elegant style with a long, sweeping tail on the final letter.

Raina Rose Tagle

Senior Associate Vice President and Chief Risk Officer

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state

Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Iowa residents, State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Pro-Tem, Inc. dba PTI Systems is located at 2525 South Shore Boulevard, Suite 401 League City, TX 77573.

For Massachusetts residents, You have the right to obtain a police report if you are the victim of identity theft.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.