STANFORD UNIVERSITY
OFFICE OF AUDIT, COMPLIANCE AND PRIVACY
Room 10, Encina Hall, 616 Serra Street, Stanford, CA 94305-6212
Phone: 650/725-0074, Fax: 650/725-0073

June 16, 2016

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Breach Notification

To Whom It May Concern:

Pursuant to N.H. Rev. Stat. 359-C:19 et seq., I am writing to inform you that on April 4, 2016, Stanford University discovered that a third-party vendor's on-line system (W2-Express operated by Equifax) had been breached using social security numbers and dates of birth of employees and former employees to improperly access, and in some cases use, W2- information. The information compromised included the following:

- First name
- Last name
- Social Security Number
- Address
- Wage information
- Tax information

We have not been able to determine the exact date of the incident, although it likely began in late January or early February of this year. Once the incident was identified, the on-line site was promptly disabled. In addition, we have reported the incident to the FBI and the IRS for investigation. Two (2) residents from the State of New Hampshire were notified of this breach, which included the offering of 24 months of credit monitoring services from two (2) different agencies.

At Stanford, we take the privacy and security of personally identifiable information very seriously. We continue to investigate this matter internally, and to enhance our systems and practices to prevent similar occurrences in the future. Please contact me if I can provide additional information on this matter.

Sincerely,

DR Moyer

D. Richard Moyer
Associate Vice President, Audit, Compliance & Privacy

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
- 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

AllClear ID

Information about Identity Theft Prevention

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to $5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

AllClear ID

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:

Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and

- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

EQUIFAX®

About the Equifax ID Patrol identity theft protection product

ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies. Note: You must be over age 18 with a credit file in order to take advantage of the product.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax, Experian**, and **TransUnion** credit reports
- Wireless alerts and customizable alerts available (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report™ (available online only)
- Up to $1 million in identity theft insurance with $0 deductible, at no additional cost to you †
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert placement with automatic renewal functionality* (available online only)

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go to www.myservices.equifax.com/patrol

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.
4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: www.fraudalerts.equifax.com or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

Form **14039** (April 2016)	Department of the Treasury - Internal Revenue Service **Identity Theft Affidavit**	OMB Number 1545-2139

Complete this form if you need the IRS to mark an account to identify questionable activity.

Section A - Check the following boxes in this section that apply to the specific situation you are reporting *(Required for all filers)*

☐ 1. I am submitting this Form 14039 for myself

☐ 2. I am submitting this Form 14039 in response to a mailed 'Notice' or 'Letter' received from the IRS. If person in **Section C** received IRS 'Notice CP 2000', or other IRS Notice questioning income, follow the instructions on that IRS 'Notice' or 'Letter'.
- Please provide 'Notice' or 'Letter' number(s) on the **line to the right** _____

☐ 3. I am submitting this Form 14039 on behalf of my dependent.
Please complete **Section F** on reverse side of this form.
Caution: If you are filing this on behalf of a Minor or Dependent, filing this form will protect his or her tax account but it will **not** prevent the dependent in **Section C** below from being claimed as a dependent by another person.

☐ 4. I am submitting this Form 14039 on behalf of another person *(other than my dependent)*.
- Please complete **Section F** on reverse side of this form.

Section B – Reason For Filing This Form *(Required)*

Check only **ONE** of the following boxes that apply to the person listed in **Section C** below.

☐ 1. **Federal tax records affected** and I am a victim of identity theft

☐ 2. **Federal tax records not affected** and I am a victim of identity theft, or an event has affected/compromised my personal information placing me at-risk to be a future victim of identity theft.

Please provide an explanation of the identity theft issue, how you became aware of it and provide relevant dates.

Section C – Name and Contact Information of Identity Theft Victim or Potential Victim *(Required)*

Taxpayer's last name	First name	Middle initial	**Taxpayer Identification Number** *(Please provide your 9-digit SSN or ITIN)*

Current mailing address *(apartment or suite number and street, or P.O. Box)* If deceased, please provide last known address.

City	State	ZIP code

Tax Year(s) in which you experienced identity theft *(If not known, enter 'Unknown' in one of the boxes below)*								**Last tax year a return was filed**

Address used on last filed tax return *(If different than 'Current')*	**Names used on last filed tax return** *(If different than 'Current')*

City (on last tax return filed)	State	ZIP code

Telephone number with area code *(Optional) If deceased, please indicate 'Deceased'*	Best time(s) to call
Home telephone number Cell phone number	

Language in which you would like to be contacted ☐ English ☐ Spanish

Section D – State or Federal Issued Identification *(Required)*

Submit this completed form and a **clear and legible** photocopy of **at least one of the following** documents to verify the identity of the person listed in **Section C** above. **If necessary, enlarge photocopies so all information is clearly visible**.

Check the box next to the document(s) you are submitting:

☐ Driver's license ☐ Social Security Card ☐ Passport ☐ Valid U.S. Federal or State government issued identification**

** Federal employees should not copy his or her employee identification cards as 18 U.S.C. prohibits doing so.

Section E – Penalty of Perjury Statement and Signature *(Required)*

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this Form 14039 is true, correct, complete, and made in good faith.

Signature of taxpayer, or representative, conservator, parent or guardian	Date signed

Section F – Representative, conservator, parent or guardian information *(Required if completing Form 14039 on someone else's behalf)*

Check only **ONE** of the following five boxes next to the reason you are submitting this form

☐ **1. The taxpayer is deceased and I am the surviving spouse.** *(No attachments are required, including death certificate)*

☐ **2. The taxpayer is deceased and I am the court-appointed or certified personal representative.**
Attach a copy of the court certificate showing your appointment.

☐ **3. The taxpayer is deceased and a court-appointed or certified personal representative has not been appointed.**
- o Attach copy of death certificate or formal notification from a government office informing next of kin of the decedent's death.
- o Indicate your relationship to decedent: ☐ Spouse ☐ Child ☐ Parent/Legal Guardian ☐ Other _____

☐ **4. The taxpayer is unable to complete this form and I am the appointed conservator or have Power of Attorney/Declaration of Representative authorization per IRS Form 2848.**
- o Attach a **copy** of documentation showing your appointment as conservator or POA authorization.
- o If you have an IRS issued **Centralized Authorization File (CAF) number, enter the nine-digit number**:

☐ **5. The victim or potential victim is a 'minor'. 'Minor' as defined per the state in which 'minor' resides.**
By checking this box and signing below you are indicating that you are an authorized representative, as parent, guardian or legal guardian, to file a legal document on the child's behalf.
- o Indicate your relationship to minor: ☐ Parent/Legal Guardian ☐ Fiduciary Relationship per IRS Form 56 ☐ Power of Attorney ☐ Other _____

Representative's name		
Last name	First name	Middle initial
Last four digits of Representative's Taxpayer ID number	Representative's telephone number *(include area code)*	

Representative's current mailing address *(apt., suite no. and street, or P.O. Box)*

City	State	ZIP code

Instructions for Submitting this Form

Submit this to the IRS via **Mail** or **FAX** to specialized IRS processing areas dedicated to assist you. In **Section C** of this form, be sure to include your Social Security Number or Individual Taxpayer Identification Number in the 'Taxpayer Identification Number' field.

Help us avoid delays:
Choose one method of submitting this form either by Mail or by FAX, not both. Please provide clear and readable photocopies. Note that 'tax returns' may not be submitted to either the mailing address or FAX number provided below.

Submitting by Mail	Submitting by FAX
• **If you checked Box 1 in Section B of Form 14039, are unable to file your tax return electronically because the primary and/or secondary SSN was misused, attach Form 14039 and documentation to your paper tax return** and submit to the IRS location where you normally file your tax return. **If you have already filed your paper return,** submit this Form 14039 and documentation to the IRS location where you normally file. Refer to the 'Where Do You File' section of your return instructions or visit IRS.gov and input the search term 'Where to File'. • **If you checked Box 1 in Section B and are submitting this Form 14039 in response to a notice or letter received from the IRS,** return this form and documentation **with a copy of the notice or letter** to the address contained in the notice or letter. • **If you checked Box 2 in Section B of Form 14039 (no current tax-related issue),** mail this form and documentation to: **Internal Revenue Service** Fresno, CA 93888-0025	• **If you checked Box 1 in Section B of Form 14039 and are submitting this form in response to a notice or letter received from the IRS that shows a reply FAX number**, FAX completed Form 14039 and documentation with a copy of the notice or letter to that number. • **Include a cover sheet marked 'Confidential'.** If no FAX number is shown on the notice or letter, follow the mailing instructions on the notice or letter. • **If you checked Box 2 in Section B of Form 14039 (no current tax-related issue)**, FAX this form and documentation toll-free to: **855-807-5720**

Privacy Act and Paperwork Reduction Notice

Our legal authority to request the information is 26 U.S.C. 6001. The primary purpose of the form is to provide a method of reporting identity theft issues to the IRS so that the IRS may document situations where individuals are or may be victims of identity theft. Additional purposes include the use in the determination of proper tax liability and to relieve taxpayer burden. The information may be disclosed only as provided by 26 U.S.C. 6103. Providing the information on this form is voluntary. However, if you do not provide the information it may be more difficult to assist you in resolving your identity theft issue. If you are a potential victim of identity theft and do not provide the required substantiation information, we may not be able to place a marker on your account to assist with future protection. If you are a victim of identity theft and do not provide the required information, it may be difficult for IRS to determine your correct tax liability. If you intentionally provide false information, you may be subject to criminal penalties. You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by section 6103. Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can write to the Internal Revenue Service, Tax Products Coordinating Committee, SE:W:CAR:MP:T:T:SP, 1111 Constitution Ave. NW, IR-6526, Washington, DC 20224. Do not send this form to this address. Instead, see the form for filing instructions. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.