

Social Security Number Breach and IRS Tax Fraud Frequently Asked Questions

Last updated April 1, 2015.

Disclaimer: The following is compiled for your information and is believed to be accurate. Please contact senate@tamu.edu with corrections or additions.

What happened?

According to the University, an employee improperly published the Social Security numbers and first and last name for 4,697 faculty and graduate assistants who taught [or were instructors of record] during the Fall 2014 semester to a University website on February 13, 2015. The University removed the document from the website March 8th.

What is the University's response?

On March 10th the University emailed exposed employees a recommendation to file a Fraud Alert with a credit reporting agency. On March 11th the University emailed exposed employees that the University would offer them at no cost to the employee one year of LifeLock identity misuse monitoring service. On March 12th the University emailed exposed employees instructions for obtaining one year of LifeLock identity misuse monitoring service at no cost to the employee. On April 1st the President extended LifeLock coverage to two years, authorized release time to recover from identity theft, and stated that the Provost's Office would supply additional one-time resources in recovering from identity theft related to fraudulent tax returns. Click [here](#) to see the President's April 1st email.

How do I confirm whether or not my Social Security number was exposed in this breach?

If you did not receive an email March 10th or 11th you may contact Ms. Alberta Ortiz-Ganem at (979) 845-4016 or alberta@tamu.edu. She will determine if your information was released. If it was, then she will send information to help you initiate fraud-monitoring protection.

How do I file a Fraud Alert with credit reporting agencies?

Contact any one of these:

- Equifax: 800 525-6285; www.equifax.com; P.O. Box 740231, Atlanta, GA 30374-0241
- Experian: 888 397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
- TransUnion: 800 680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

The company you file a Fraud Alert with will notify the other two companies. **Important! If a Fraud Alert or Credit Freeze is in place you may not be able to set up online accounts with IRS or the Social Security Administration, so do those steps first (see below)!**

You may also request one free credit report per year from each credit reporting agency. By

timing your requests and rotating the agency, you can receive a free credit report every four months; by alternating with your spouse it is even possible for one of you to receive a free credit report every two months.

What does a Fraud Alert accomplish?

You will be contacted by a credit reporting agency if anyone (including you) requests a credit report, to confirm it was you. You will also receive fewer pre-approved credit card offers during the Fraud Alert period.

How long does a Fraud Alert last?

Ninety days per request. After it expires you may request another Fraud Alert for another ninety days.

What is the Faculty Senate's response?

Beginning with the initial notification made by the University on March 10, 2015, the Faculty Senate Executive Committee has been continuously engaged with the University administration to help faculty deal with this data breach.

The most recent meeting was March 30, 2015, with Interim President Hussey, Provost Watson, and Shane Hinckley, Interim Vice President for Marketing and Communications.

The Speaker of the Faculty Senate, Jim Woosley, emails all faculty (not just the ones exposed in this instance) with the latest information as he receives it.

How can I set up online access to view my Social Security account?

Follow the steps at <https://secure.ssa.gov/RIL/SiView.do>. Note that under some circumstances online access may not be available. **You should do this *before* placing a Fraud Alert or Credit Freeze on your credit reports.**

How can I block access to my Social Security account?

Follow the steps at https://secure.ssa.gov/acu/IPS_INTR/blockaccess.

Can I get another Social Security number?

If your identity is stolen and misused, then *after* you have pursued all other avenues to restore your identity you may apply to the Social Security Administration for a new Social Security number (see <http://www.socialsecurity.gov/pubs/EN-05-10064.pdf>).

What about fraudulent income tax returns?

If your identity is stolen it could be used to file a fraudulent income tax return with the Internal Revenue Service (IRS). To reduce this risk IRS recommends you set a PIN

at <https://sa.www4.irs.gov/irfof-efp/start.do> for your and your spouse's Social Security numbers. You can also see a transcript of what returns have been filed in your name at <http://www.irs.gov/Individuals/Get-Transcript>. **You should do this *before* placing a Fraud Alert or Credit Freeze on your credit reports.**

If a fraudulent tax return has been filed you should notify the University Police Department at <http://upd.tamu.edu> or (979) 845-2345 as well as IRS.

To notify IRS of actual or potential identity theft, file the form at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. The IRS Identity Protection Unit is at <http://www.irs.gov/Individuals/Identity-Protection>, or call (800) 908-4490. However, note that according to <http://www.washingtontimes.com/news/2015/mar/31/irs-ignoring-60-percent-taxpayers-calls/>, IRS currently answers fewer than forty per cent of calls.

Additional IRS resources are at:

- <http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>
- <http://www.irs.gov/pub/irs-pdf/p5027.pdf> (Identity Theft Information for Taxpayers)

Whom else should I notify?

The Federal Trade Commission (FTC) has primary federal responsibility for identity theft issues; they can be contacted at <http://www.ftc.gov>, (877) 438-4338, or 600 Pennsylvania Avenue N.W., Washington, DC 20580.

What University rules apply?

Rule 29.01.03.M1.24: Information Resources – Notification of Unauthorized Access, Use, or Disclosure of Sensitive Personal Information (<http://rules.tamu.edu/PDFs/29.01.03.M1.24.pdf>).

How have other universities responded to Social Security number breaches?

- According to the University, most universities they have contacted have offered one year of credit monitoring service.
- The University of Texas at Austin's standard policy is two years, at an estimated cost of \$19 to \$31 per person (http://www.utexas.edu/sites/default/files/10-14-2011_mtg_notes.pdf).
- The University of Maryland provided five years (<http://www.umd.edu/datasecurity/>).

For more information please contact:

- Joseph P. Pettibon II, (979) 845-8260
- Office of the Provost, (979) 845-4016
- Office of the President, (979) 845-2217