# Information regarding IRS tax fraud

Although tax fraud and identity theft are topics in the media daily, these criminal acts are especially prevalent when filing Federal and State tax returns. You have to look no further than our own community for individuals who have been victims of tax fraud. If you have been a victim of a fraudulent tax filing in the past we know how frustrated and victimized you can feel!

As a result, we wanted to take this opportunity to remind everyone of some best practices to help prevent tax fraud. Moreover, if you believe that you have been a victim of tax fraud, it is important that your first priority is to work with the IRS in following the instructions they have provided for you. IT IS IMPORTANT FOR YOU TO RE-FILE YOUR TAX RETURN ACCORDING TO THEIR INSTRUCTIONS. The following is a link of their instructions: https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft

If you believe you are a victim of identity fraud and it is affecting your federal tax, such as your attempt to file your federal tax return electronically was rejected, or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended you:

- Contact your tax preparer, if you have one;
- File an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf);
- Call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm);
- Report the situation to the local police department. Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection.

No one can ever know for sure how a single individual's identity has been breached. The following information is being provided to help you avoid becoming a victim of tax fraud and provide guidance if you already are a tax fraud victim:

***How could someone else get my tax/social security information?***

The IRS estimates this year they will pay out over $21 billion dollars in fraudulent returns and some estimate that 1 in 4 tax filers has experienced this in the past couple of years. Most Americans do not realize their social security number already exists on the black market at a sale price of $1-$3. These numbers have been obtained from a variety of sources over the past decade as part of massive security breaches. These include, but are not limited to:

Target, Amazon, Citibank, BCBS Anthem, Experian, Turbo Tax, Department of Veterans Affairs, Ebay, the Voter Database and countless other large organizations. The following link shows some of the largest breaches in the past 10 years:

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

In the past, your SSN has been provided to every bank, dr., hospital, school, credit card application, even the cable company. Many of these have had significant breaches over the past 10 years. The IRS itself had tax returns stolen for several years before discovering the breach. Last spring, the PIN numbers they assigned to prior year tax fraud victims were hacked and those numbers also stolen.

Last tax season the IRS issued an alert that hackers are now able to break into most tax preparers' software without their knowledge. IN OTHER WORDS… Tax fraud is big business and the thieves are located all over the world…even our own back yard. Two years ago a large cell in Milwaukee was uncovered and participants arrested. This group in particular targeted companies in the Midwest. Usually, the thieves can go undetected for long periods of time.

If that isn't enough, professional thieves can discover your social security number within a short time period…most estimate as quickly as 25-30 minutes.

Did you know that the first 5 numbers of your social security card are not specific to you but rather where you were born and your age? Both of these data points are easily found on search engines online or in your very own social media postings. Once they have these 5 numbers, an algorithm can run a program and search for the last 4 digits until there is a match with your name.

***How do the thieves often operate?***

The easiest method used is downloading a prior years' tax return from the many breaches that occurred from 2010-2015. However, that isn't the only way this happens.

Per security experts, some will target a geographical area. They will search for the largest employers in the area and then secure names belonging to that employer. Once they have the names, everything else is fairly easy. This has been the case in the Holland area as the organizations/businesses being targeted the most are some of the county's largest employers.

***Has our Hope College computer system been breached?***

Our CIT Department watches daily for attempts to break into our system and at this time we are not aware of any breaches of our data. We do know that colleges and their employees are targets with last year almost every college in Michigan and many across the country experiencing IRS fraud at some level. How can this be? Security experts indicate the primary source is colleges have online directories with employee names. Once they criminals have a list of names, they simply can match it up to other information for sale, or run a program to find the information they need. In tracking the number of our employees impacted each year, our numbers coincide with what would be considered "expected" activity.

***What can I do now?***

First, you should follow the steps the IRS has instructed you to follow using the link above.

Other precautionary measures you can take to help protect your personal information include placing a Fraud Alert on your credit files. You can place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

If you are concerned about becoming a victim of fraud or identity theft, you may also request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

| | | |
|---|---|---|
| Equifax Security Freeze | Experian Security Freeze | TransUnion Security Freeze |
| PO Box 105788 | PO Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |
| https://www.freeze.equifax.com | http://experian.com/freeze | http://www.transunion.com/securityfreeze |
| 1-800-685-1111 | 1-888-397-3742 | 1-800-680-7289 |
| Equifax | Experian | TransUnion |
| P.O. Box 105069 | P.O. Box 2002 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |
| www.equifax.com | www.experian.com | www.transunion.com |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |

Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. If you believe an unauthorized third party has your bank account, we encourage you to talk with your bank regarding steps they suggest to protect it.

Moreover, under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. After you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission

(FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount. For additional information, please see Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

Utilize the account monitoring services provided by your bank(s) and credit cards. A text or email will be sent when transactions occur that exceed dollar amounts or if on-line transactions are charged to your credit

You should also take steps to notify any institution where you have financial transactions that your social security number has been breached.

***Should I get an Identity Theft policy?***

That is up to you but policies such as LifeLock do watch for use of your identity. You can purchase various levels of policies. Realize that once they have attempted to file a fraudulent tax return they will most likely try again next year. The IRS system does seem to be catching them earlier this year.

***Can I do anything to help with next years' tax return?***

File early! Those who typically file prior to mid-Februray do not have as many issues although the criminals seem to file earlier every year. Although this isn't possible for everyone, if you can, file early! Retrieve your tax documents online with your financial institutions if you haven't received all your statements via mail. Banks, mortgage companies etc. will often have this information online prior to mailing their statements.

***Anything else?***

We hope that you find the above useful and encourage you to take steps to protect your information. Our CIT department continues to monitor our systems at the College and issues alerts when they see suspicious activity. To date that has been predominantly phishing schemes in our email systems.

We also ask that your report any fraud to the HR department as we continue to monitor levels. Increases in these numbers could indicate a change in methods being used. And keep steadfast! You are not alone in this!