

US Tax Refund Method

Well as you know 2014 tax season is here so you know what that means

TAX RETURNS

This is a very easy method to do and by the end I am sure you will be wondering why more people do not know about it.

It is gaining media attention this year (specifically in FL) and I suspect that within 1-2 yrs the USA legislators will take the steps necessary to close the loopholes in the tax code so this method will at the very least be much more difficult to reproduce. Currently e-file returns undergo little or NO review process at all before the refunds are sent out.

W2's are not matched from the employer to the return until several weeks AFTER the close of tax season (far too late to catch discrepancies). The best way to protect yourself from any situation is to know exactly what happens, so you will receive information below which is going to show you for EDUCATIONAL PURPOSES ONLY what a criminal does to fraudulently obtain a tax refund under someone else's info which should help you protect yourself from such theft.

Scammers need the following:

- 1) Fullz Info (name, dob, ssn and address)
- 2) Drop address (foreclosed home, home for sale, rental home, abandoned house or verified drop service) – address can be different from that of the previous tax returns since the return is verified with the AIG PIN from the previous year confirming the address.
- 3) VPN, Proxy, Sock5, public computer access (wifi also works) -5socks.net
 - Check your IP address in system anti fraud detections, detecting real location will display the users current IP info including whether or not the connection is flagged, blacklisted, etc.
 - Socks can be found on the forums easily. Or via vendors.
- 4) Clean email such as hushmail, created while VPN is active! Email is always accessed via secure/anonymous connections and never without first clearing all cookies/cache.

Scammers first gain access to fullz info (name, dob, ssn and address, sometimes filing status). This is very easy to do thru carding forums, employer databases, hacked dbs, inmate dbs, SSN (deceased) dbs, etc. With this info they file w2 federal returns before the SSN holder has a chance to do their own (legitimate) taxes, thereby receiving a fraudulent refund prior to that person receiving theirs. Younger filers return fewer errors since there is less chance of a mismatch on filing status when obtaining the PIN than with older people who may be divorced, married filing separate, married joint filing, etc. When the AIG PIN is confirmed there is little to worry about (IRS allows 3 tries to get AIG pin info right, then locks out the SSN from further attempts. A rejection could be due to bad address, dob or filing status or a combination.) If the SSN is rejected, a new one must be attempted.

To stay protected the scammer will use a VPN service (such as cryptocloud, which is the best VPN available and keeps no logs) which accepts anonymous payment such as LR or money service such as MG or WU. Alternatively they may use proxies, public computer access or SOCKS5 to mask their IP address. This is to prevent any IP logs when filing thru turbotax (TT) or when requesting AIG PIN via IRS website. It's best to pay for any service (CryptoCloud included) via a secure line, anonymous PC or stolen wifi).

The users will either file thru the IRS e-file directly or file thru the TurboTax website via the free federal EFILE method. TT offers the advantage of a step by step method, cutting down on time so a scammer can complete a return in as little as 30 minutes. This method works so well for them because the IRS doesn't verify the submitted tax return prior to sending out the refund, in a way (as some news articles stated) the IRS becomes an unwitting accomplice in the matter by having such lax controls. Within 72 hrs of receiving confirmation of a good return, the IRS sends the refund automatically.

The scammer will turn on their VPN, proxy, SOCK5, etc prior to starting to ensure a clean connection (cookies cleared, cache cleared, new window open, check IP address via IP-score, etc). The best way to operate is with VPN on, and on top of that, use Sock5 in the browser for whatever state you're filing. This makes TT think you're filing in that state. They start by taking the account information and verifying the AIG PIN prior to starting. If the AIG PIN isn't available the return can't be filed and the rest of the work would be a waste of time. In some cases an error will be

returned stating there is no PIN, that is OK it just means the person didn't file a return in the prior year in which case the scammer will check "NO 2012 RETURN FILED" during the return process.

First the scammer verifies the SSN is good by obtaining the AIG PIN (this is the pin verifying the filer is in fact the person whose SSN is being entered). The AIG PIN can be requested via <https://sa1.www4.irs.gov/irfofefp/start.do> (ON A SECURE CONNECTION) if the filer cannot remember their Gross Adjusted Income (AIG) from the previous year.

Once verified the scammer creates a profile of the person and creating a TT profile and beginning the guided process. It is not necessary to save the info as it is entered as it only takes 10mins per return on avg. At the end of the return TT requires a profile be created prior to submitting. This is what the throwaway email is for.

Fill out name

- 1- Select filing status (this is known already from obtaining AIG PIN).
- 2- Next enter address used for drop service (does not have to match previous records)
- 3- Enter phone (doesn't have to be valid though they can use Google voice, forwarding service etc if someone wants to have access to calls regarding the return).
- 4- Scammer marks the state of residence as the state where the person's refund is headed. Since the IRS does not verify W2s until several weeks AFTER the tax deadline, the refund has already been sent out by the time the IRS realizes an error was made.
- 5- Enter birthday of person's full
- 6- NO – cannot be claimed as dependant
- 7- No disabilities
- 8- Enter SINGLE
- 9- Not a student
- 10- Gives this result to the scammer
"We're combing through hundreds of deductions and credits and you qualified for one so far:
Your personal tax exemption"
- 11- No, didn't make money in other states
- 12- No kids to support
- 13- SSN entered
- 14- Confirm finished with personal info
- 15- Skip upgrade
- 16- Select WORK ON MY W2 now
- 17- Here the scammer needs an EIN (Employer ID #) 9 digit #. They obtain these either through the records they have or by entering a spoof EIN found on services such as FEINSearch.com. You can also search google for EINs but a real EIN is a MUST and it MUST match the address on file for the EIN or the return will be rejected.
- 18- Enter the address of the employer
- 19- Now starts working on wages. Typically wages under \$50k would produce fewer flags, fraud screens, irregularity checks, etc. Anything below \$108,000 means that the boxes 1, 3 and 5 have the same value. Many scammers play around with these numbers. Each prepaid refund card has a daily withdraw limit of \$2,500 and a daily

spend limit of \$3,500. Lower refunds are NOT A BAD IDEA for scammers since the card can be used quick and disposed of easily. \$25k wages should produce refund of about \$5k.

20- Federal tax withholding (BOX 2) is usually entered at 35% (the default federal withholding for taxpayers subject to federal tax withholding) – on \$25k that's roughly \$7k withheld totaling a \$5k refund). Since federal taxes are far below the default 35% withholding, the scammer receives the difference in the form of a refund!

21- BOX 4 SS withholding is 4.2% of wages.

22- BOX 6 Medicare withholding is 1.45% of the wages.

23- If there is a state income tax, it is withheld in the appropriate box when they have selected a state where personal income is taxed at the state level (some states have no income tax). This can be inflated as well. States without income tax:

Alaska

Florida

Nevada

New Hampshire

South Dakota

Texas

Tennessee

Washington

Wyoming

24- Boxes 7, 8, 10, 11 are left blank. 25- Rest of boxes left blank

26- Deductions – NO DEDUCTIONS AT ALL, there are no taxes to be paid so deductions are useless.

27- Federal standard deduction is displayed as automatically selected deduction – accept.

REVIEW – will show refund

28- Review Results

Should show "Congratulations" message.

29- SKIP state return if filing in state without income tax (as previously noted)

30- Click wrap up tab – continue – continue – at this point the scammer receives the refund total displayed onscreen.

31- Continue again past state tax

32- Skip protection (LOL)

33- Continue

34- Print and file – DON'T PRINT – just file. Select EFILE

35- EFILE NOW

36- Chance to DOUBLE my refund and select to receive the prepaid debit card

37- Sign the form (sometimes there may be an error with the SSN or eligibility to receive the prepaid card, in which case an error message will appear. Unless the scammer opts to receive paper check, start new return. This almost never happens.

38- Skip cell phone, the scammer then enters the email they created earlier.

39- Finish the confirmation steps and EFILE (the scammer gets an email confirming it) and within a day or so another email confirming it was accepted. Within 72hrs the refund can be tracked on the IRS website. Cards take 7-10 days to arrive though they can come sooner so the drop must always be monitored.

That's it!!! Now the scammer is going to wait 7-10 days to receive the card in the mail. SEE HOW EASY THIS IS?!?! Once a carder gets the hang of it they can file them in 10mins or less!!

The alternative to getting a TT prepaid card is this. The scammer first checks an AIG PIN for validity of a full. Then he/she goes to a site like netspend.com where they will send a reloadable visa to any drop free of charge (fee is paid on first load with direct deposit). Once signed up they are provided a routing and acct# which they enter into the TT software for a DIRECT DEPOSIT (2 days faster) so that by the time the "clean" card comes in the mail its ready to be activated and already has the refund on it.

---NOTE: the account holder of the card MUST MATCH EXACTLY the name on the return. So each card is good for only ONE RETURN.

DO NOT buy in store cards (CCTV, activating in store, etc), just not advised.

Regarding TT prepaid cards:

The maximum amount that can be spent on your Card per transaction is \$2,500.00, with a maximum total of \$3,500.00 in transactions per day, including both purchases and cash withdrawals. The maximum value of your Card is restricted to \$10,000.00. You may use your Card to purchase or lease goods or services wherever Visa debit cards or Interlink cards are accepted as long as you do not exceed the value available on your Card Account.