

Identity Theft: Who's Got Your Number?
Hearing Before the Senate Finance Committee
Statement of Rebecca Spencer
April 10, 2008

Thank you, Chairman Baucus and Ranking Member Grassley, for this opportunity to share my experience regarding tax related identity theft with the members of the Senate Finance Committee.

In 1975, I took over a home based tax practice with about 1600 clients from my uncle. Since that time the business has grown to over 6500 tax clients annually. As an Enrolled Agent, I have always been a strong supporter of e-file; in fact, my office was the first e-filer in the State of Montana.

At first, e-filing was very restricted, with identity checks and compliance visits to all Electronic Return Originators (EROs). I felt quite secure that my client data was not something an identity thief could use. Since that time, e-filing has been opened up to the entire world. Anyone with a little prior planning can take a laptop into a cyber café with a stolen identity, including a valid employer identification number, and file a United States income tax return.

On January 14th of this past year, three days after e-file opened, one of my long time clients came to the office and filed her tax return. She usually filed in February but this year she was in desperate need of the money. The following morning, instead of a refund loan check, we got an IRS acknowledgement that her return had already been filed. Someone had used this single, financially struggling mother of two's identity and filed a tax return on January 13, well before most people get around to filing.

My client was in tears and I realized we had a real case of identity theft on our hands. Not knowing who to call in the IRS, I started with the Criminal Investigation 800 number. The recording there states, "If you would like to file Form 3949A [an Information Referral to report tax fraud] please order this form by calling 1-800-IRS-FORM. This form can also be ordered on our web site at www.irs.gov". There was not even an option to leave a name and phone number or wait for a representative.

I called the IRS e-help desk at the Service Center and their response was: "She will have to mail in a paper return."

Next, I sent my client down to the local IRS walk-in center, where she was told to file a paper return. As an Enrolled Agent, I felt that because the taxpayer's name and social security number were on the return she should have been entitled to a transcript - but the IRS refused. *She was denied access to her own tax account.* The walk-in office could not help until she gave them a social security card, driver's license, birth certificates, a letter of explanation and a written copy of the police report (which took

several days to get). After that, she was referred to yet another IRS function, the Taxpayer Advocate Service, which eventually was able to resolve her case.

The taxpayer was worried that her children's identities had also been stolen, but the IRS could tell her nothing until after she waited for the police report. I called the refund loan bank and was able to find out that the thief had filed as single without dependents, worked for a major US employer, had filed on-line, and applied for a refund loan credit card (a stored value card) instead of a check. (It is my understanding that with the stored value card the thief can go to an ATM with the password, thus avoiding the need for fingerprints or picture identification.)

The bank had not given the loan because the withholding was too high on the W-2. After my call to the bank, the return was flagged and when the tax refund arrived at the bank the money was held until the IRS was able to decide which taxpayer was legitimate.

Bottom line: *Ten days after the Internal Revenue Service had been notified that there was a problem, the Service released a refund to the fraudulent taxpayer.* It was only because I called the bank and gave them a heads-up about the identity theft that the refund was held up and not issued to the fraudulent taxpayer – *not because of anything the IRS had done to stop it.* Two months later, after contact with at least four IRS functions, the victim, with the help of the Taxpayer Advocate's Office, finally received her tax refund.

My office gets calls early in the tax season asking to prepare the return from a final pay stub. When we tell them we are unable to do so they say, "I'll just do it myself on the internet." (Another entire subject is how easy it is to print anyone's W-2 off the internet.) A taxpayer who is not following the rules only needs last year's employer identification number to file early. Among these early filers are the thieves filing a return with a stolen identity.

These returns are a financial drain on the system because they result in audits, amended returns which must be filed, or, as would have been the case had the bank not held the fraudulent deposit, outright loss of the refund amount.

My client had her identity stolen as a result of the theft of a government credit card. Another client had his wallet stolen. Identity theft can happen to anybody under the most normal of life's circumstances.

Several possible safeguards come to my mind:

- 1) Require the W-2s to be turned into Treasury electronically prior to being given to employees instead of one month later.
- 2) Do not open e-file to the general public on the internet until the W-2s are required to be in the taxpayer hands.

- 3) Annually give each employer a two letter code that must be included on the W-2 and require the code be entered on the e-filed return. This would prevent thieves from using prior year W-2 information to file fraudulent returns.
- 4) Have the taxpayers not using paid preparers fax their W-2 to the IRS or have them scan it into the software. Back in the days when we filed paper, everyone waited until they received a W-2 that they attached to the return. The dishonest weren't so prone to add an extra digit to the IRS withholding.
- 5) Have available a special mail stop for Electronic Return Originators or better yet have a way for irregular returns to actually go through electronically and *automatically stop the refund* on the previously used Social Security number until the legitimate filer can be identified. At present it is my understanding that Financial Management Service has NO way to stop the transfer of funds.
- 6) Require on-line filers to enter the prior year adjusted gross income or hold the processing until AFTER the 8453 [the signature form] with W-2s attached has been received by the Service.

I am sure many if not all the above suggestions can be met with excuses as to why they cannot be implemented. I would like to remind you of the year Senator Baucus suggested social security numbers of dependents had to be entered on the tax forms. Did the IRS do anything with the social security numbers for the next ten or so years? No--- but how many dependents disappeared because the SSNs had to be reported?

The do it yourself software a presents a finished product that is difficult for the untrained eye to distinguish from a professionally prepared tax return. If the IRS issued bold easy to read warnings about preparers who do not sign returns, taxpayers who file prior to getting their W-2, and stealing identities or dependents (along with some big dollar fines connected with the practices) perhaps we would at least have taken one step in discouraging identity theft and the financial drain that results.

I believe the proposed tax practitioner registration and accompanying requirements will also help to eliminate incompetent return preparers who may be more prone to fraudulent practices.

Thank you again for this opportunity to testify and share my experience and ideas with a committee that has acted so diligently to preserve the integrity of the tax system over the years.