

Prepared Testimony
for the Record of

John C. Walker, EA

Hearing on

Tax-Related Identity Theft and Fraudulent Tax Returns

Before the

United States Senate
Committee on the Budget

Manchester, NH
August 16, 2015

Chairman Enzi, Senator Ayotte, and members of the committee, my name is John Walker, I am and enrolled agent in private practice. I was asked to testify today from the perspective of an enrolled agent and the impact tax-related identity theft and fraudulent tax returns are having on the professional community.

You may be aware, but just to be clear, there are four groups of tax professionals, enrolled agents, CPAs, attorneys, and all others preparers. Generally, enrolled agents, CPAs, and attorneys are authorized under Circular 230 to represent taxpayers before the Internal Revenue Service. There are a few clearly defined special circumstances where someone who is not an enrolled agent, CPA, or attorney may represent an individual. It is usually one of those three tax professionals to whom taxpayers turn for help when they are a victim of tax-related identity theft. Yet we are the portion of the professional community who have been most adversely impacted by tax-related identity theft. So it is with regard to that group of professionals—those regularly representing taxpayers—that I am focusing my remarks.

To put my remarks in some perspective as reflective of the professional community, I will summarize my background. I became an Enrolled Agent in 2004. Prior to that I had a thirty year career in information technology management in manufacturing companies. Since becoming an Enrolled Agent I have been a member of the National Association of Enrolled Agents (NAEA), the National Association of Tax Professionals (NATP), the National Society of Accountants (NSA), and a board member of the New Hampshire chapter of NSA (NHSA). Every month I participate in an IMRS¹ telephone conference with anywhere from 15 to over 30 other tax professionals from all over New England and New York, members of IRS stakeholder liaison, and occasionally IRS operations managers. The purpose of the conference is to discuss systemic problems identified on a national or regional level, raise new issues, learn what is being done to resolve them, and suggest solutions from the professional community. Twice a year we hold practitioner liaison meetings where two dozen tax professionals from New Hampshire meet for half a day with IRS regional and occasionally national managers. The purpose of these liaison meetings is to have in-depth and free exchange of ideas, problems, and solutions. It is from this background of interaction with other tax professionals that I am speaking.

As tax-related identity theft has escalated so have the complaints I hear over, and over, again from professionals trying to help clients who are victims of tax-related identity theft.

In its haste to respond to the explosion in fraudulent returns, the IRS has severely restricted or blocked entirely access to taxpayer information by enrolled agents, CPAs, and attorneys. Restricting representative access to information renders the taxpayer's right to proper representation meaningless.

This is happening even when the taxpayer has engaged us to assist in resolving the tax-related identity theft and named Identity Theft as a tax matter on the power of attorney. To make matters worse, I'm now hearing the same problem voiced by other tax professionals handling cases where identity theft is not a known part of the problem.

Instead of working with the professional community to speed resolution of these cases, the IRS has made it increasingly difficult, and sometimes impossible, to help our clients.

¹ IMRS is the IRS acronym for their Issue Management Resolution System, an electronic system for gathering information about and tracking resolution of problems encountered with IRS systems and procedures.

Furthermore, a taxpayer who has been the victim of identity theft is still expected to comply with all other aspects of the tax code—timely file their tax returns, pay their taxes, make estimated tax payments, continue installment payments, and fulfill any obligations agreed to as part of an offer in compromise. To assist a taxpayer with any problems arising with those other compliance matters, as well as to assist directly in resolving the identity theft, we as tax professionals representing the taxpayer still need access to all the same information we would have if the identity theft had not occurred.

Normally a representative would have online access to a client's tax information using a professional tool provided by the IRS. This tool differs dramatically from the Get Transcript function that posed a problem earlier this year. It would not be helpful to go into the technical differences on a public record, but it is more secure. It is similar to the kinds of systems many of us rely on to manage our personal bank accounts, utility payments, credit card accounts, insurance, student records, and the like.

Unfortunately, a representative's online access is now blocked for any taxpayer where an ID theft has been reported, and in some cases, it is blocked where ID theft is simply suspected, or might be possible. This delays or stops the tax professional from assisting the victim in determining what happened, and when. It is also causing serious delays in resolving even some of the most routine tax matters, and in tax years unaffected by the year in which the fraudulent return was filed.

What makes this all the more frustrating for taxpayers and representatives is that, a taxpayer or representative, or someone posing as either, can call IRS customer service, then sit on hold for an hour or two. When their call is finally answered a customer service agent will read, mail, or fax the same information to the caller.

Even in those cases where a customer service agent asks a representative to fax over their power of attorney, this process is absurd. For it bypasses the individual electronic keys a representative must have to obtain information online. Those keys are unique to that representative and known only to that representative.

Thus, the same information that a representative could have obtained on their own in five or ten minutes, now consumes hours of Service and professional time to produce. This is a serious waste of Service telephone and human resources, as well as professional resources, and it is a completely misguided sense of improving security.

One specific suggestion I can offer is that the IRS should be doing exactly the opposite. Insist that any representative who needs to obtain copies of IRS records must go through the process of registering and being validated to use the online tool to get them. Require representatives use the online tool, and stop releasing information with telephone requests.

I'll give you a parallel example. Recently I needed a copy of an older statement for my personal bank account, one that was no longer available online. There were only two ways I could obtain a copy, show up at a bank branch with photo ID and they would print it there, or log into my online account, answer several security questions, then submit the request electronically and it would be mailed to the address currently on record. What the IRS is currently doing is the equivalent of any one of you being able to obtain a copy of my bank statement simply by calling and giving my account number which you obtained from a discarded deposit slip or a check I once wrote.

Enrolled agents, CPAs, and attorneys are individuals who have made a substantial investment in obtaining and maintaining a professional license. We are known to and have been vetted by our respective licensing authorities, often including a criminal background check and fingerprinting. We know our clients personally, usually for many years and sometimes for decades. We know the details of our client's financial history. We have more information in our files about our clients than the IRS has; we have to have it to substantiate the returns we prepare. We could easily provide information to help the IRS quickly and efficiently to establish who the real taxpayer is, and separate the return that is real from the one that is fraudulent. Instead, the IRS is telling ID theft victims it will take six months to a year while the IRS investigates to identify who is the real taxpayer. Meanwhile, the taxpayer is left in limbo for a grossly unreasonable length of time struggling to put their financial life back together.

This delay is all the more absurd when you consider that even in this post 9/11 era the Department of State can determine the true identity of an individual with a sufficiently high degree of confidence to issue them a United States passport in just four to six weeks. If you expedite it, a passport can be issued in two to three weeks. Furthermore, the State Department does it without the benefit of the detailed financial history the tax professional community could bring to the process of identifying the correct tax return. If the Department of State can move that quickly, why can't the IRS do it?

In a case of tax-related ID theft the first priority the IRS should pursue is to establish the identity of the true taxpayer. Why not take the very simple and obvious step of telling the taxpayer to go to a local IRS office and present their passport? It has the taxpayer's photo, full name, place of birth, and date of birth. If the taxpayer doesn't have a passport they can get one in far less time than it takes the IRS to even get its investigation off the ground. If necessary, their identity can be further substantiated with details of their financial history from their tax professional.

Once the identity of the correct taxpayer is established, the IRS can issue the taxpayer unique PINs for their returns. The victim and the IRS can move forward saving a vast amount of time and resources for the Service and suffering for the victim.

Several further examples of the difficulties the professional community experiences in trying to work with the IRS on tax-related identity theft can be found in the events that have occurred in a case I am currently working.

Chris and Jane Stevens (not their real names) are a New Hampshire couple in their early 60s. Chris and Jane got in serious financial difficulty after getting over extended on their mortgages, using the money to try to keep a small company alive during the failing economy and manufacturing jobs in New Hampshire. The Stevens ended up in bankruptcy it drag on for several years until their bankruptcy plan was finally accepted last August. 2014.

In late February 2015 they received a check in the mail from Sunrise Bank in California in the amount of \$9,855. The accompanying paperwork explained that it was for their 2014 federal tax refund of \$9,945 less \$90 for a tax preparation services and bank fees. The letter went on to explain that the bank was unsuccessful in direct depositing the refund to the bank account specified on the return and therefore was mailing a paper check.

The Stevens immediately knew that something was wrong because we had not yet even begun to prepare their 2014 return. They also knew that their identities had been among those

stolen in the Anthem data breach which had occurred earlier that month. Jane quickly called me and we prepared the necessary Identity Theft Affidavits and filed them with the IRS.

I began investigating how the fraudulent funds could be returned successfully to the U. S. Treasury and properly credited to the Stevens' account. I reached out to one of my contacts in IRS Stakeholder Liaison for help in answering this question. After about a month of research she was successful in locating the name and address of an IRS office in Fresno, California where we could send the check.

On April 15, 2015 we mailed the check with a cover letter explaining the situation and including all possible identification information. It was sent via USPS Priority Mail with signature confirmation. Within a few days we received the name, signature and ID number of the person who signed for it. We also timely filed the Stevens 2014 return following the special instructions for paper filing returns where ID theft has been reported.

It is worth noting in this case that the total tax withheld from the Stevens wages was nowhere near \$9,945. They actually have a balance due on their 2014 return. Further, they have a substantial tax debt that survived their bankruptcy. Any 2014 refund, whether real or fraudulent, should have been stopped and offset against that tax debt. In this case, the tax refund system failed opportunities to protect Treasury interests.

In the first week of August 2015 the Stevens received a call from a revenue officer in Holtsville, New York. I returned the call on their behalf and learned from the revenue officer she wanted the Stevens to return the check. I explained to her that the check had been sent to California in April as instructed, and had been signed for by the IRS. She insisted that it had never been returned, or if it was, it had been lost, and there was no record of it in the system. After further debate she agreed to let me fax over copies of everything that have been sent to California and the signature confirmation of its receipt. The fax was sent within the hour and the success of the fax transmittal confirmed.

I find it odd that the revenue officer specifically asked for return of the physical check, not repayment of an erroneous refund. She had to have had some reason to know the check had not been cashed and to think that after six months the Stevens were simply sitting on a \$9,855 check.

Two or three days later I called the revenue officer to follow up. She claimed she never received the fax so she had sent the case to exam so they could pursue my client for the money. That was the extent of that revenue officer's willingness to work the case assigned to her and help resolve the taxpayers' problem.

A few days later the Stevens received a letter, this time from the Kansas City campus, demanding they either return the check or pay the \$9,855 by September 3, 2015.

Since then Jane Stevens and I have both spoken with the fraud department at Sunrise Bank. We have learned the check was never cashed. After returning the check to California it was either lost or the IRS simply did nothing with it; the IRS never contacted the bank.

We also learned the funds are still in the account at Sunrise Bank. The bank has a process to return unclaimed funds to the IRS but it will take at least 15 days and requires cooperation from the IRS to accept the return of funds. On Jane's request the bank has begun that process but it will not be completed by September 3, 2015, nor in the interim can the bank provide us with any written confirmation that they are in fact attempting to do that.

However, there is one bizarre twist to the return process that the bank warned me about. Before they can return the funds to the IRS, the bank is required to try again to deposit them to the bank account designated by the thief on the fraudulent return. If that second attempt is successful the money will be gone.

The IRS does have authority to subpoena bank records and investigate that account and the authority to levy the funds in that account. The fraud department told me they would cooperate fully with the IRS but it is the responsibility of the IRS to initiate either or both actions.

This case is ongoing and I remain optimistic it will be resolved successfully. From the events that have occurred so far it is clear that neither the taxpayers nor I have received any help, guidance, or cooperation from any of the IRS operating groups who are supposed to be addressing tax-related identity theft. The only real help we received came from a very dedicated individual in IRS Stakeholder Liaison and the fraud department at Sunrise Bank.