Statement of Mike Kasper

June 2, 2015

Dear Members of the Committee:

On Friday, February 6, I filed my taxes by using the desktop version of Turbo Tax like I do every year. However, later that evening I got an email notice from Turbo Tax that the IRS had rejected my return because a federal tax return had already been filed by someone else using my social security number.

On Monday morning, February 9, I called the IRS identity theft hotline who confirmed my identity with tax related questions and then told me a direct deposit was being made for a tax refund filed with my social security number on that same day, into a bank account different than any that I had used before. Obviously, I knew and they agreed this was fraud, but they said it was too late to stop the deposit now. In addition, since I was alerting them this transaction was fraudulent, their privacy rules prevented them from giving me any more information, such as the routing number and account number of that deposit.

When I asked why, they all but admitted it was to protect the privacy of the criminal, not because they were going to investigate it right away. If I had played dumb and just asked what account my deposit was going into they probably would have told me. Yet because I was straightforward and told them it was fraud, they would not tell me, even in person at the IRS office. They were clear, my case would not be investigated further until a fraud affidavit and accompanying documentation were processed by mail. They said if I had filed a day earlier and called on Friday, they could have just stopped the deposit, but because it was being paid they could not tell me more, or call the bank, until it was fully investigated.

The most interesting thing to me about this rule is that the IRS itself refuses to look at the bank account data until it is fully investigated. Banks are required by law to report suspicious refund deposits, but the IRS does not even bother to contact banks to let them know a refund deposit was reported fraudulent, at least in the case of individual taxpayers who call, confirm their identity and report fraud, just like I did. The IRS told me it can take six months to investigate. Meanwhile, an unknown criminal has all my data.

Frustrated by not knowing who stole my identity, I then tried to get a transcript of the fraudulent return online using the Get Transcript function on IRS.gov on the same day, February 9, but I soon learned that someone else had already registered their email address for my social security number. When I called IRS eServices to fix this, and spent another hour on hold, they explained they could not tell me what the email address was either, due to privacy regulations, but something about the email address led them to believe that is was not me and it seemed suspicious. They said they could not change the email address, all they could do is ban access to eServices for my SSN. It was unclear if they would investigate further.

Regardless, I was able to successfully ask the IRS for a copy of the fraudulent tax transcript sent by mail, which I got a few weeks later. It did not show the deposit account number, but showed whoever filed it had access to my 2013 tax return, because the amounts were very similar and they knew a lot about me. Eventually, by looking around the IRS website, I discovered that I could submit Form 4506 and pay $50 for a photo copy of the fraudulent return, which I did. Just $50 and they would ignore the privacy rules.

On March 17, I obtained the photo copy of the fraudulent return in the mail which showed the bank account information and I saw the fraudulent return was submitted January 31, 2015, with a corrected W-2 that had increased the withholding by exactly $6,000 to increase their total refund due to $8,936.

On March 18, I contacted First National Bank of Pennsylvania whose routing number was listed, and reached their head of account security who called back and confirmed a direct deposit by the IRS for $8,936.00 was made on February 9, 2015 into someone else's checking account, but specifying my name and my social security number in the meta data with the deposit. She told me that she could also see that transactions were made at one or more branches in the city of Williamsport, PA to withdraw those funds and a substantial portion of the money was gone. She also told me that no one from the IRS had contacted her bank to raise any questions about that deposit, despite my fraud report filed February 9. She said she was required to report it to the IRS herself now, and would cooperate with local police too.

At this point, I finally had some progress, a chance to find my ID thief. So I called the Williamsport police and spoke to the Lieutenant who heard my story and sympathized with the lack of any investigation by the IRS. He asked me to write out my story in an email to his Captain, which I sent to them on March 19. About two hours later, I received a call from an investigator who had been assigned to work on my case. He followed up March 20 with the bank, then interviewed the person who held the account and told me the bank's fraud department was investigating it now too, and had asked the woman to return the cash.

It seemed like my case was basically solved. However, it turned out to be more complex. At least if you believe the story that the account holder is telling. According to her, she herself had been conned. She said she responded to a Craigslist ad about a money making opportunity. Money was deposited into her account, and she sent money to individuals in Nigeria through Western Union, keeping some as a profit, and apparently never suspecting that she might be doing something illegal. I'd like to believe her story, but wouldn't someone who could pull this off also have an explanation ready? Apparently she received the refund for someone from South Dakota as well and I believe that a warrant is out for her arrest now. Regardless, I believe that being able to get a copy of the return for $50 and contacting the bank did help to resolve my case. Just over 90 days after I filed, I got my full tax refund check in the mail on May 12. Several days later, I received a letter from the IRS stating that my identity theft case was confirmed and that I would receive an Identity PIN at the end of the year to use when filing my taxes next year in 2016.

The GAO found millions of people experience stolen ID refund fraud and $5.8 billion is lost each year. By contrast 5,000 banks are robbed and $6,000 lost on average. This fraud equals 1 million bank robberies. If the IRS cannot handle all of this fraud, redact any unrelated third party SSNs and mail taxpayers copies of returns to pursue it themselves with local law enforcement or banks, like I did successfully in my case. USPS is the preferred means of communication for the IRS so they need to use it more to help taxpayers.

Last but not least, why does the IRS rely on a few multiple choice questions to safeguard tax transcripts? E-filing PINs are even easier to get. It is so simple to file a false tax return for a refund it is actually giving criminals an incentive to attempt more data breaches, since they can trade SSNs for cash from the IRS. I understand putting government services online provides significant cost savings, but it needs to be done securely to avoid actually costing more to reverse all the damage done by criminals committing ID theft. Computer security requires a more advanced approach today than it did five years ago. It is no longer enough to put up strong filters and firewalls and depend on them holding. You have to assume criminals will find a way around them and actively monitor all systems like the immune system does in our bodies. I'm not an expert on fraud, but I believe a lot more can be done to protect taxpayers and to prevent this.

Sincerely yours,

Mike Kasper