Comments of Chairman John L. Valentine,
UTAH STATE TAX COMMISSION

To

U.S. Senate Finance Committee
March 12, 2015

Mr. Chairman and esteemed members of the Senate Finance Committee, I come before you this morning to discuss and recommend actions that can be taken to reduce the contagion of tax fraud which is sweeping the country.

There are four issues for your consideration this morning:

1. Strengthen information sharing between the IRS and the States.

2. Stricter regulation of the financial industry as it relates to "pre-paid" debit cards.

3. Prohibit the practice of applying refunds to payment of fees for filing services, a practice sometimes called "Refund Transfer."

4. Require third party filing services to tighten front end security by using multi-factor authentication and other measures to secure data from unauthorized disclosure and identity theft.

Prior to the commencement of the 2015 filing season, Utah installed a state of the art computer software system to identify potentially fraudulent returns. On January 20 of this year, the Utah Tax Commission opened filing of income tax returns and deployed this system. As we began to process returns, our system started sending out verification letters to taxpayers whose returns appeared suspicious. Within ten days of the opening of the filing season, we began receiving calls from taxpayers who had received our communication about their return; they had not yet filed their returns.

We initially thought these were isolated incidents, but they were not. As that week progressed, our software identified more and more suspicious returns. We found several factors that were the same in all the suspicious returns:

- All the suspicious returns had the direct deposit information changed from the previous year's bank account to prepaid debit cards, often Green Dot brand debit cards.

- All the suspicious returns contained routing and account numbers that differed between the federal return and the state return.

- Most of the suspicious returns appeared to have the exact 2013 tax return data populated to the fraudulent 2014 return.

- The address on the suspicious returns was the same as the address on the 2013 return.

- Since most of these filings were being made through the Turbo Tax system, it appeared that something in their process was compromised.

After communicating with the owners of Turbo Tax, (Intuit), and notifying other states through our national organization, we notified the Internal Revenue Service of the possible compromise of the Modernized Electronic Filing (MEF) systems. The accounts in question were immediately sent to the IRS for review. On February 10, 2015, we sent 31 returns to the Ogden IRS Service Center that we had verified by contact with the taxpayers as being fraudulent. As of the date of this testimony, the IRS has not contacted us with the results of any determinations on their part of the nature of the returns. They did inform us in a phone conversation that they had known about a filing scheme which took a previous year's return and copied it into a current year's filing. The IRS representative stated that they had known about this scheme since last year, but had not notified the states of this fact.

Many have asked what action was undertaken by the state of Utah when it discovered this attack. In short, we hurried.

- We stopped all refunds until we could analyze the magnitude of the problem.

- During the first week, we identified five different repeating fraud schemes.

- We identified the returns with specific characteristics that were potentially fraudulent.

- We deployed our identity quiz system and commenced sending "ID verification letters" on the returns that met the unique characteristics of potential fraud.

- If the taxpayer failed the quiz, they were instructed to send us certain documentation to verify their identity, that included:

  Two forms of identification such as SSA card, passport, drivers license, state ID card, government issued photo ID, utility bill, bank statement, payroll stub, college transcript or insurance policy, and

  One picture ID.

- If the taxpayer does not respond to the quiz or fails to provide the needed information, the system will reverse the return as though it had not been filed.

- To the extent we could identify them, refund deposit requests to pre-paid debit cards have been converted to a paper warrant (check) and sent to the taxpayer's address.

As we continue to prevent the outflow of fraudulent refunds, we found great difficulty in determining the nature of financial institution routing and account information. We specifically found that there was no uniformity in numbering to distinguish traditional checking accounts and savings accounts from prepaid debit cards. For example, a prepaid reloadable debit card sold by Green Dot, appears to be linked to a bank account even though the debit card had no actual checking or savings account associated with it. (These cards may even appear as a Visa or Master Card.) Quoting from their card holder's agreement: "Your card is a prepaid debit Visa or MasterCard card, which means that you must add funds or "load" your card in order to use it. There is no credit line associated with your Card." Once the funds are transferred to such cards, they cannot easily be traced or recovered, a perfect vehicle to commit fraud. A simple fix would be to require a different series, letter or additional numbers to distinguish these cards from cards connected to bank or credit union checking and savings accounts.[i]

To obtain a Green Dot re-loadable prepaid Visa or MasterCard debit card, a customer is required to provide their name, address, date of birth, Social Security number, phone number, and other information that will allow Green Dot to identify customers.[ii] If a Green Dot customer is pretending to be someone else by assuming that person's identity, then the identity thief has successfully obtained a fraudulent method to gain access to resources or other benefits in that person's name without the use of a traditional bank account. Perpetrators then use these fraudulently obtained pre-paid debit cards to make thousands of dollars' worth of retail purchases, quickly cash them out or drain them at an ATM. Prepaid debit cards appear to be preferable to fraudsters because the identity thief doesn't have to bother with banks, credit unions or check-cashing stores that may become suspicious when one person starts bringing in multiple tax refund checks to be cashed or deposited.

While we progressed though the investigation, we found a practice that enables fraudsters to perpetrate fraud without having anything at risk, a practice called "refund transfers." Here is how it works: The fraudster is allowed to deduct the third party filing fees from the refund. The third party filing service gets paid, the fraudster receives the refund and the state and federal government (and potentially the taxpayer who may actually be entitled to a refund) are out the funds.

Finally, we found third party filing services often lack the front end security measures necessary to protect their users in this cyber world. At a minimum, these services should install multi-factor authentication to assure that a person filing a tax return is indeed the person identified on the return. Quality fire walls and other data protections are a given, but since we are uncertain at this time of how the prior return information was obtained, it is a careful company, concerned about their product and its customers, that will invest the funds necessary to protect their data from cyber thieves.

[i] An ABA routing transit number is a nine digit code which identifies the financial institution on which it was drawn. It was originally used to facilitate sorting, bundling, and shipment of paper checks back to the drawer's (check writer's) account. As new payment methods were developed (ACH and Wire), the system was expanded to accommodate these payment methods.

Unfortunately, prepaid debit cards cannot be specifically identified by routing numbers or bank account numbers using the present standardized methods. A standardization of routing or account numbers to include identification of prepaid debit cards would facilitate evaluation of suspicious filers and enhance the ability of Federal and State taxing authorities to deny refunds to the fraudsters and catch fraudulently filed income tax returns.

[ii] Green Dot maintains that it is compliant with Federal money laundering laws and with all Patriot Act elements.