WRITTEN
TESTIMONY OF
KENNETH C. CORBIN
COMMISSIONER, WAGE AND INVESTMENT DIVISION
AND
SILVANA GINA GARZA
CHIEF INFORMATION OFFICER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
ON THE FAFSA DATA RETRIEVAL TOOL
MAY 3, 2017

INTRODUCTION

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to discuss the work being done to secure the online Data Retrieval Tool (DRT) that is accessible from the fafsa.gov and StudentLoans.gov websites.

The IRS works continuously to safeguard our systems and protect taxpayer information. An important focus of this work is the ongoing battle against stolen identity refund fraud. We have made steady progress over the last few years in stopping fraudulent refund claims, criminally prosecuting those who engage in this crime, and helping minimize the adverse effect on taxpayers.

Despite all the progress we have made, the threat is constantly evolving. Fraudsters and criminal enterprises are using complex and highly sophisticated tactics to reach their target. As the IRS improves its capabilities and shuts off certain avenues of entry, identity thieves look for new ways of getting in. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals attempt to become more sophisticated at faking taxpayers' identities. We know we cannot rest and that solutions we implement are only good until the thieves find a new way to circumvent our defenses. We must stay diligent and ever watchful.

To address this challenge, the IRS is working not just to react better and faster, but to anticipate the criminals' next moves and stay ahead of them. To that end, we have used funding provided by Congress to increase our monitoring, detection, and analytical capabilities in relation to suspicious activity within our systems. These improvements have helped us slow down identity thieves, but we still need to do more. Congress helped us in this regard by approving $290 million in additional funding in 2016, which included $95 million to improve cybersecurity. We used a portion of that funding to implement the use of monitoring equipment and other capabilities that are more sophisticated than

what we had used previously. This has helped us detect suspicious activity in our various online tools and applications more quickly.

We have also undertaken a broad effort to review the authentication practices for programs where we share taxpayer information, and strengthen those practices where necessary.

One example of this effort was our decision last year to eliminate the electronic filing Personal Identification Number (e-file PIN) as an option for taxpayers to use to verify their identity when filing their tax return. Taxpayers received the e-file PIN by entering certain identifying information into an electronic tool on IRS.gov. After discovering unauthorized attempts had been made to obtain e-file PINs using data stolen from sources outside the IRS, we halted use of the e-file PIN. Although our analysis of the situation found that no personal taxpayer data was compromised or disclosed by IRS systems, we believe it was necessary to discontinue the e-file PIN to protect taxpayers and their data.

Our efforts to strengthen authentication practices also extend to programs where the IRS is authorized to share taxpayer data with organizations that use it to verify eligibility for customers who apply for loans. Since last summer, we have been working with banks, mortgage companies, and others to ensure they were implementing strong “know your customer” requirements.

Along those lines, in June 2016, the IRS announced new, stronger requirements for participants using the Income Verification Express Service (IVES). IVES is used by pre-screened companies who, in turn, are hired by mortgage firms and loan companies that need to verify applicants’ income. Going forward, the IRS will only accept requests for taxpayer data from IVES participants who certify that they are using the new requirements to verify their clients. We took this step out of an abundance of caution to protect taxpayer information as well as safeguard IVES, which has been a successful program for the government, taxpayers, and the private sector since 2006.

THE FEDERAL STUDENT AID DATA RETRIEVAL TOOL

Applying for student financial aid is another area where we are concerned about the potential for bad actors to obtain taxpayer information fraudulently. We are working with the Department of Education to secure the online process through which student financial aid applicants obtain their federal tax information, which they need to complete the *Free Application for Federal Student Aid* (FAFSA®) or apply for an income-driven repayment (IDR) plan for their student loans. The focus of our concern is the Data Retrieval Tool (DRT), which allows an applicant to automatically populate the FAFSA, or an IDR plan application, with the required information from the applicant’s tax return.

In the fall of 2016, we had an early indication of a potential misuse of the DRT to access taxpayer data. While the attempt was not successful, it highlighted the possibility that, with stolen personal information, a bad actor could pose as a student, begin completing an online application for student aid using the FAFSA, and give permission for the IRS to populate that application with tax data using the DRT.

Although the attempt failed, we immediately advised the Department of Education of our concern that criminals could access the tool and fraudulently obtain taxpayer data. We explored several potential solutions to address these concerns.

At the time, we agreed with the Department of Education that since we had no evidence of confirmed criminal activity and given that cutting off the tool could potentially increase the application burden for a large number of students and parents, we would not shut down the DRT immediately, but monitor usage, while we explored solutions that would meet both of our needs. We made this decision with the understanding that further action would be necessary if any indication of criminal activity was identified.

In early 2017, the IRS's Cybersecurity Fraud and Monitoring team observed anomalous behavior on the Federal Student Aid DRT using the IDR application. The IRS immediately increased monitoring and blocked Internet Protocol (IP) addresses based on the suspicious activity observed. The Department of Education performed additional analyses on the suspicious activity and determined that it was not fraudulent attempts to access tax data from the IRS.

Shortly thereafter, we learned of an incident that led us to determine that there was evidence of identity theft and likely fraud. Based on this incident, the IRS cybersecurity team was able to identify a pattern of suspicious activity. The pattern indicated criminals, having obtained personal information from sources outside the IRS, were masquerading as applicants for student financial aid and using the DRT to obtain enough tax return information to allow them to file fraudulent tax returns. The data obtained through the unauthorized use of the tool were later used, in some instances, in an attempt to file fraudulent returns. Having confirmed that the activity was fraudulent, we decided to turn off the DRT.

STEPS TO HELP TAXPAYERS

The IRS is working to identify the number of taxpayers affected by questionable DRT use. We are also continuing to review the extent to which this contributed to fraudulent tax returns. We have identified some instances where our strengthened fraud reviews stopped a significant number of questionable tax returns by filers who accessed the DRT.

Our investigation of unauthorized attempts to access the DRT found that approximately 100,000 individuals may have had their taxpayer information compromised. We have mailed letters to these taxpayers to alert them to the possibility of suspicious activity related to their personal information, and to offer them free credit monitoring.

Along with notifying these taxpayers, the IRS is also marking their accounts to provide additional protection against the possibility that an identity thief could file a false return using their information. We are also giving these taxpayers the opportunity to obtain an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years.

The roughly 100,000 taxpayers identified as potentially affected by this incident includes approximately 8,000 for which a return has been filed and a refund issued. We are analyzing these returns to determine if any of them are fraudulent.

IMPROVING E-AUTHENTICATION FOR THE DRT

The original IRS authentication process set up for DRT users to verify their identities was standard at the time the DRT was developed in 2009. This required users to provide their first and last name, Social Security Number (SSN), date of birth, tax return filing status, and address of record. .

We conducted an e-authentication risk assessment, completed last fall, which indicated the need for strengthened authentication procedures. Since then, we have worked collaboratively with the Department of Education to determine how best to strengthen these procedures, both for our DRT and their online FAFSA and IDR plan applications.

In working with the Department of Education, we recommended several potential solutions. We first looked at short-term solutions, but none of the ones proposed met all of the security requirements that we identified. The longer-term solutions we explored included the following:

- Strengthening user authentication protocols to a level to prevent unauthorized users from viewing tax return data using the DRT;
- Randomizing or obscuring the AGI and other data fields in such a way that what is viewed is not an exact depiction of the applicant data to be transmitted, making it less useful to criminals;
- Masking and encrypting the information so that the applicant would not be able to view it, but could still transmit it to the Department of Education;
- Exploring a legislative change to Internal Revenue Code section 6103 that would authorize the Department of Education to receive the data directly from the IRS, which would greatly increase security.

After consulting with the Department of Education we decided that, in the absence of legislation, the most effective solution would be to mask and encrypt the data, as envisioned in the encryption solution mentioned above, so that the data would not be visible to the applicant, thereby shielding information from last year's tax return from anyone masquerading as the student applicant. Randomizing or obscuring the information would not provide sufficient protection, and increasing the authentication procedure would make the tool unavailable to most applicants.

The option we chose balances the need to protect the taxpayer data while trying to make the solution accessible to the students applying for financial aid. The IRS is working toward an operational system upgrade for the IDR application by late May or early June 2017. The encryption upgrade is also planned the for 2018–19 FAFSA launch on October 1, 2017.

In the interim, families can still complete applications for student financial aid by manually providing the requested financial information from copies of their tax returns. And, if necessary, they can obtain a copy of those returns either online through the Get Transcript application, by mail, or from their tax preparer. Although we realize this is more burdensome than using the DRT, we have a responsibility to protect the DRT and all of our online tools from identity thieves. We will continue to discuss with the Department of Education other options for long-term solutions that ensure that the FAFSA remains accessible to everyone who wants to pursue postsecondary education while protecting sensitive taxpayer data.

Chairman Chaffetz, Ranking Member Cummings and Members of the Committee, that concludes our statement. We would be happy to take your questions.