HEARING BEFORE THE
OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

"Reviewing the FAFSA Data Breach"

Testimony of
Timothy P. Camus
Deputy Inspector General for Investigations
Treasury Inspector General for Tax Administration

May 3, 2017

Washington, D.C.

TESTIMONY
OF
TIMOTHY P. CAMUS
DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

"Reviewing the FAFSA Data Breach"

May 3, 2017

Chairman Chaffetz, Ranking Member Cummings, and Members of the committee, thank you for the opportunity to testify about the 2017 criminal exploitation of the Free Application for Federal Student Aid (FAFSA) and Data Retrieval Tool (DRT).

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 to help maintain the integrity in America's tax system. It provides independent audit and investigative services to improve the economy, efficiency, and effectiveness of IRS operations. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA plays the key role of ensuring that the approximately 83,000 IRS employees[1] who collected more than $3.3 trillion in tax revenue, processed more than 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2016,[2] have done so in an effective and efficient manner while minimizing the risk of waste, fraud, and abuse.

TIGTA's Office of Investigations investigates allegations of IRS employee criminal and administrative misconduct, attempts to threaten or harm IRS employees, facilities or IRS data infrastructure, and external attempts to corrupt tax administration through the impersonation of IRS employees and programs, taxpayer data exploitation, and attempts to bribe IRS employees.

For the purposes of this hearing, my testimony will focus on the protection of taxpayer information, specifically the 2017 exploitation of the FAFSA application and the DRT.

---

[1] Total IRS staffing as of January 7, 2017. Included in the total are approximately 16,200 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2016*.

RECENT CHALLENGES IN SECURING TAXPAYER DATA

As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information will continue to be a top concern for the IRS and for TIGTA. According to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, Federal agencies reported 77,183 cyberattacks in FY 2015, an increase of approximately 10 percent from FY 2014. The increasing number of data breaches in the private and public sectors means more personally identifying information than ever before is available to unscrupulous individuals.

Due to the $400 billion dollars the IRS issues in refunds and the 242 million tax returns it processes each year that contain extremely valuable information for identity thieves, the IRS has become a favorite target of cyber criminals located all over the world. For example, in May 2015, criminals launched a coordinated attack on the IRS e-Authentication portal that resulted in the exploitation of the IRS Get Transcript Application, as well as the IRS IP PIN application. It is estimated that more than 110,000 taxpayers were impacted by this attack.

A subsequent review of all of the activity on the system revealed that more than 700,000 taxpayers were impacted by similar abuses of the system by multiple bad actors over an extended period of time. In January 2016, a coordinated effort was launched that exploited the IRS Electronic Filing PIN (e-File PIN) tool. The e-File PIN tool was created to provide taxpayers with a special PIN number that would allow the taxpayer to electronically file a Federal tax return. The IRS estimates the exploitation resulted in the issuance of over 100,000 e-File PINs that were used to file over $100 million dollars of fraudulent tax returns. As a result of this exploitation, on June 23, 2016, the IRS announced that it had disabled the e-File PIN application. Numerous investigations are underway on the individuals who obtained taxpayer information from both of these attacks.

FAFSA AND THE DRT

The DRT allows students and parents to access their adjusted gross income (AGI) information through an interface with the IRS to complete the FAFSA by transferring the AGI information directly into their FAFSA application form. FAFSA on the web was first introduced in on June 30, 1997 and the IRS DRT component of the process was activated on January 28, 2010.

Following the e-Authentication Get Transcript exploitation in May 2015, the IRS reevaluated the authentication risk on outward-facing online applications based on today's known cyber-crime environment. The IRS conducted this e-Authentication Risk Assessment (eRA) on 45 applications, including the FAFSA and DRT process. On October 25, 2016, the IRS determined the risk factors involving financial loss or agency liability, harm to agency programs or public interests, and the risk of unauthorized release of sensitive information utilizing the FAFSA and the DRT were all scored in the low risk category. On December 5, 2016, the Risk Assessment Form and Tool was signed by the IRS, and the FAFSA and DRT remained operational.

It appears that identity thieves used personal information of individuals that they obtained outside the tax system to start the FAFSA application process in order to secure the AGI tax information through the DRT. The IRS' current estimate for the number of impacted taxpayers is approximately 100,000. TIGTA is conducting a joint investigation of this exploitation with IRS Criminal Investigation and the Department of Education Office Inspector General (Education OIG). As part of our investigation, we are also looking back to see if there was an earlier bulk exploitation of the FAFSA and the DRT process. TIGTA is also planning to initiate an audit to review this issue.

In September 2016, TIGTA detected an attempted access to the AGI of a prominent individual. When we investigated the attempted access, we determined that the FAFSA application and the DRT were used in this attempt. Since FAFSA is a Department of Education application, we notified the Education OIG and we notified the IRS Privacy, Governmental Liaison and Disclosure (PGLD) program office. We initiated a joint investigation with the Education OIG that included the Cyber Crimes Task Force. The investigation identified the individual responsible for the attempted access and he was arrested. This case is still proceeding through the court system. In November 2016, we noticed another attempted access of the same prominent individual's AGI through the FAFSA and the DRT, this time, from an entirely different location. We have included this attempted access in our investigation activity and we also notified the PGLD program office. This activity is still under investigation.

On January 25, 2017, the IRS reported to us that a high number of Taxpayer Identification Numbers were being processed through FAFSA and the DRT. The IRS told us that when they shared this observation with the Department of Education, Education told the IRS that they believed the activity was related to student loan consolidation activity.

On February 27, 2017, a complainant reported that he received a copy of his tax transcripts at his home with a letter telling him that he had requested them. The complainant reported he never ordered a copy of his tax transcripts. When his tax account information was researched, we learned that the complainant's AGI had been accessed through the FAFSA and the DRT process. As a result, we determined that the January activity that the IRS observed was proof that an exploitation was under way. Initial analysis showed there were 8,000 questionable accesses at that time.

On March 3, 2017, the IRS reported that they disabled the DRT due to privacy concerns and to protect sensitive taxpayer data.

We are continuing our criminal investigations of this activity and are reviewing evidence and information obtained from the investigations of the prior e-Authentication exploitations to determine if the FAFSA and DRT criminal activity was launched by the same individuals and groups. In one instance, we found evidence that as far back as February 2016, the subject of an e-Authentication investigation discussed the availability of AGI information using FAFSA and the DRT. After comparing additional log file information and email addresses, we now have very good indications that in some instances, the same individuals and groups engaged in criminal activity on the e-Authentication portal are involved in this exploitation of the FAFSA and the DRT.

We at TIGTA take seriously our mandate to provide investigative coverage of issues that confront the IRS in its administration of our Nation's tax system. As such, as we conduct our investigations of the criminals who are responsible for the cyber exploitations, we share the information we find with the IRS in order to help protect the IRS' data infrastructure. We plan to provide continuing coverage of the IRS' efforts to operate free from criminal activity in the electronic environment.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to share my views.