



# AMERICANS FOR LIMITED GOVERNMENT FOUNDATION

---

10332 MAIN STREET · NO. 326 · FAIRFAX, VA 22030 · PHONE: 703.383.0880 · FAX: 703.383.5288 · WWW.GETLIBERTY.ORG

December 14, 2015

CC:PA:LPD:PR (REG-138344-13)  
Room 5203  
Internal Revenue Service  
POB 7604  
Ben Franklin Station  
Washington, DC 20044

Via online submission

**Re: Comment on Notice of Proposed Rulemaking on Substantiation  
Requirement for Certain Contributions**

To Whom It May Concern:

I write today to provide the comments of Americans for Limited Government Foundation (ALGF) on the Notice of Proposed Rulemaking (NPRM) referenced above. The ALGF is a non-profit organization that is recognized as exempt from taxation under Section 501(c)(3) of the Internal Revenue Code (IRC). As such, the NPRM affects not only ALFG, but every other similarly situated entity.

As an initial matter, the NPRM makes clear that no regulation is needed in this area and therefore the NPRM is truly a solution in search of a problem. In fact, the NPRM states,

The present CWA system works effectively, with minimal burden on donors and donees, and the Treasury Department and the IRS have received few requests since the issuance of TD8690 to implement a donee reporting system.<sup>1</sup>

Based on this admission, the public in general and the regulated community in particular should be puzzled to say the least as to the reasons why the IRS is now

---

<sup>1</sup> Substantiation Requirements for Certain Contributions, 80 Fed. Reg. 55,802, 3 (September 17, 2015) (to be codified at 26 C.F.R. pt. 1.)

proposing this regulation. The IRC Section, Section 170(f)(8)(D) that provides the authority to promulgate regulations regarding a return with donee information was passed as part of the Omnibus Budget Reconciliation Act of 1993. Now, greater than two decades later, the IRS has decided to promulgate a regulation that it admits isn't necessary and is not required.

Section 170(f)(8)(D) of the IRC states,

Substantiation not required for contributions reported by the donee organization. Subparagraph (A) shall not apply to a contribution if the donee organization files a return, on such form and in accordance with such regulations as the Secretary may prescribe, which includes the information described in subparagraph (B) with respect to the contribution.

This section, while providing the authority for an alternative means of substantiation, does not require the IRS to promulgate a regulation. It may, however, promulgate a regulation, provided that it shows that the regulation is necessary. As will be shown by the analysis that follows, and the fact that the current system has operated just fine for over two decades, the IRS has failed to demonstrate that the regulation is necessary.

## **The NPRM is an Open Invitation to Identity Theft**

### **IRS Problems with Data Security**

As the IRS knows very well, it has a bad track record when it comes to protecting taxpayer information and taxpayers have suffered as a result.

This year it was revealed that at least 100,000 individuals had personally identifiable information from past tax returns stolen from the IRS, "using the IRS's own website."<sup>2</sup> This information was used to file fraudulent tax returns with the IRS and enabled the thieves to direct tax returns to accounts controlled by them.<sup>3</sup> These thefts occurred despite knowledge on the part of the IRS that their data security practices were inadequate to protect taxpayers' information.<sup>4</sup>

---

<sup>2</sup> Opening Statement of Chairman Ron Johnson, "The IRS Data Breach: Steps to Protect Americans' Personal Information," U.S. Senate Committee on Homeland Security and Governmental Affairs, June 2, 2015. Available online at: <http://www.hsgac.senate.gov/hearings/the-irs-data-breach-steps-to-protect-americans-personal-information> (accessed December 14, 2015).

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

Although the IRS was made aware of the weaknesses in its authentication practices as early as March, according to Commissioner Koskinen the IRS made a conscious decision to not make any changes to its authentication practices.<sup>5</sup>

The IRS has been warned numerous times by the Treasury Inspector General for Tax Administration (TIGTA) about the dangers posed by its data security practices. In October of last year TIGTA noted,

Computer security has been problematic for the IRS since 1997. In April 2014, the Government Accountability Office (GAO) reported that the IRS is making progress in addressing information security control weaknesses; however, the GAO noted that weaknesses remain that could affect the confidentiality, integrity, and availability of financial and sensitive taxpayer data.<sup>6</sup>

In 2013 TIGTA found,

During our audit, TIGTA determined that eight (42 percent) of 19 PCAs [planned corrective actions] that were approved and closed as fully implemented to address reported security weaknesses from prior TIGTA audits were only partially implemented. These PCAs involved systems with taxpayer data.<sup>7</sup>

In 2011 TIGTA found,

TIGTA found that non-mainframe databases containing taxpayer data were not always configured in a secure manner and that databases were running out-of-date software that no longer receive security patches and other vendor support.

In addition, the IRS had not fully implemented its plans to complete vulnerability scans of databases within its enterprise. Also, the IRS purchased a database vulnerability scanning and compliance

---

<sup>5</sup> *Id.*

<sup>6</sup> Memorandum for Secretary Lew from J. Russell George, Treasury Inspector General for Tax Administration, October 15, 2014, at p. 3. Available online at: [https://www.treasury.gov/tigta/management/management\\_fy2015.pdf](https://www.treasury.gov/tigta/management/management_fy2015.pdf) (accessed December 14, 2015).

<sup>7</sup> *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data*, Treasury Inspector General for Tax Administration, September 27, 2013, at p. 2. Available online at: <https://www.treasury.gov/tigta/auditreports/2013reports/201320117fr.pdf> (accessed December 14, 2015).

assessment tool without the completion of adequate product evaluation and testing.<sup>8</sup>

In 2010 TIGTA found,

Current processes were not effective at identifying all contractors who receive IRS taxpayer data and are subject to required security reviews. The Infrastructure Security and Reviews (ISR) office identified contractors that require reviews by asking IRS business organizations to identify their contractors that process, store, or house IRS taxpayer data. However, this process did not identify all contractors who have been provided such data. Without an effective process for identifying the contractors receiving IRS taxpayer data, the IRS cannot ensure that all contractors who receive such data are being reviewed for compliance with security requirements. As a result, the IRS cannot ensure that taxpayer data are protected at contractor facilities.<sup>9</sup>

With all these problems it is little wonder that the data breaches discussed above occurred. Ironically, the IRS provides a page on its website with tips on what to do in the event of a data breach.<sup>10</sup>

Given that the IRS lacks the ability to adequately protect taxpayers' private information, no regulations should be promulgated which require or encourage the sending of more private taxpayer information to the IRS. If the IRS cannot secure its existing systems what assurance is there that they can build a secure new system to receive the reports that would be developed pursuant to the NRPM?

### **Data Security Problems for Tax Exempt Organizations**

In addition to the risks to taxpayer data that occur from having more of it stored in IRS computer systems, there is also a risk to taxpayers by having that data stored in the computer systems of the reporting organizations. If the IRS, a multi-billion dollar federal agency with over 90,000 employees, cannot adequately secure taxpayer data

---

<sup>8</sup> *Security Over Databases Could be Enhanced to Ensure Taxpayer Data Are Protected*, Treasury Inspector General for Tax Administration, May 4, 2011, at p. 2. Available online at: <https://www.treasury.gov/tigta/auditreports/2011reports/201120044fr.pdf> (accessed December 14, 2015).

<sup>9</sup> *Taxpayer Data Used at Contractor Facilities May Be at Risk for Unauthorized Access or Disclosure*, Treasury Inspector General for Tax Administration, May 18, 2010, at p.2. Available online at: <https://www.treasury.gov/tigta/auditreports/2010reports/201020051fr.pdf> (accessed December 14, 2015).

<sup>10</sup> *Data Breach: Tax-Related Information for Taxpayers*, IRS, undated. Available online at: <https://www.irs.gov/Individuals/Data-Breach-Information-for-Taxpayers> (accessed December 14, 2015).

then what makes the it think that a small non-profit organization will be able to do so? In order to be able to file the report with the IRS the organization must have that information stored in a computer system. This puts the organization at risk for the same type of attacks that lead to the disclosure of taxpayer information from the IRS computer systems as discussed above.

Many small non-profits would likely prefer to not keep sensitive information on donors for these reasons.

In addition to the problems faced by donors if their information is exposed, the entity holding the information may face legal complications as well. The Federal Trade Commission (FTC) has recently engaged in a series of investigations and settlements with entities that were the victims of criminal acts by third parties that resulted in those third parties obtaining access to sensitive information on the entities customers. The FTC has held that, "the statutory prohibition against unfair trade practices in Section 5 [15 U.S.C. § 45] could be applied to allegedly unreasonable and injurious data security practices."<sup>11</sup>

Problems with a federal agency going after the victim of a crime and adding insult to injury aside, the additional risks associated with housing data that may become the subject of a hacking or other illegal action by a third-party may well be enough for many non-profits to decline to house any such data. Faced with a situation where donors would be lost to the non-profit if their data is disclosed and then enforcement action from a federal agency after the fact, why would any small non-profit take the risk? These concerns will help fulfill the prophesy in the NPRM that, "donee reporting will be used in an extremely low percentage of cases."<sup>12</sup>

## Conclusion

The IRS is wasting taxpayers' hard-earned money by considering this issue. The regulation is clearly not needed, will be used little if at all, and poses numerous privacy problems. Based on the foregoing, the NPRM should be immediately withdrawn.

Sincerely,



Nathan Paul Mehrens  
President and General Counsel

---

<sup>11</sup> *In the Matter of LadMD, Inc.*, Initial Decision by D. Michael Chappell, Chief Administrative Law Judge, Federal Trade Commission Docket No. 9357, November 13, 2015, at p. 4. Available online at: [https://www.ftc.gov/system/files/documents/cases/151113labmd\\_decision.pdf](https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf) (accessed December 14, 2015).

<sup>12</sup> *Substantiation Requirements for Certain Contributions, supra*, at 55,804.