United States Senate
COMMITTEE ON FINANCE
WASHINGTON, DC 20510–6200

April 5, 2017

The Honorable John Koskinen
Commissioner
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

Dear Commissioner Koskinen:

As you know, Americans today face more cyber related threats than ever before. Although the impact of cyber fraud—such as phishing—on consumers is difficult to measure, some sources estimate over 80,000 people are affected by phishing every day. Indeed, just last year, as you know, the Internal Revenue Service (IRS) noted a 400% increase in phishing attacks in which criminals impersonated the IRS. I write to you today to ask that the IRS enable a widely-adopted cybersecurity technology that will prevent fraudsters from being able to send emails that purport to come from irs.gov.

In 2015, the information technology industry finalized a technical standard known as Domain-based Message Authentication, Reporting & Conformance (DMARC). This technology enables the administrator for an organization such as IRS to request that fake email messages impersonating that organization be quarantined in a spam folder, or rejected by a recipient's email provider.

In the two years since it was introduced, a number of companies and government agencies have embraced DMARC. Both the National Institute for Standards and Technology (NIST) and Federal Trade Commission (FTC) strongly recommend the use of DMARC. And a number of federal agencies, including the FTC, the Federal Deposit Insurance Corporation (FDIC), and the Social Security Administration (SSA), have enabled DMARC and configured it in the strictest "reject" mode, so that emails impersonating their organization are automatically rejected.

While it appears that the IRS has already enabled DMARC, it also appears that IRS has configured DMARC in a less restrictive mode. As a result, the IRS receives automatic alerts when the organization is impersonated by fraudsters, but unsuspecting taxpayers are not warned or automatically protected. If IRS could more fully enable DMARC (e.g., enable "reject" or "quarantine" modes), the email providers of potential victims would automatically reject the fake IRS emails or redirect these to a spam folder.

I am concerned that taxpayers may be needlessly exposed to phishing scams because the IRS is not taking full advantage of DMARC's capabilities. I urge you to follow the good example set by the FTC, FDIC, and SSA by enabling the strictest DMARC setting, so that email service

providers can automatically reject phishing emails purporting to have been sent from irs.gov. This simple step could drastically reduce the risk of tax-related phishing attacks. This same recommendation should apply to every federal agency, but only a few have yet acted to fully implement DMARC—so this is an opportunity for the IRS to be on the forefront of cybersecurity. I hope the IRS takes action and I appreciate your prompt reply.

Sincerely,

Ron Wyden

Ron Wyden
United States Senator