SMALL BUSINESS COMMITTEE

CHAIRMAN STEVE CHABOT
Opening Statement

SCAM SPOTTING: CAN THE IRS EFFECTIVELYPROTECT SMALL BUSINESS INFORMATION
APRIL 5, 2017

AS PREPARED FOR DELIVERY

Good morning. Thank you all for being here. A special thanks to our witness, The Honorable J. Russell George, who has taken time away from his busy schedule to be here with us today.

As tax season heats up, so too does tax **fraud** season. In testimony before this Committee last year, IRS Commissioner John Koskinen reported that a cyber breach had exposed taxpayer data from over 700,000 accounts. Commissioner Koskinen also told us that IRS computer systems are under constant attack from would-be hackers to the tune of 1 million attempted cyberattacks per day.

Criminals are becoming ever more sophisticated and ruthless in the ways they commit tax identity theft and file fraudulent returns with ill-gotten personal information. At a minimum, the goal of the IRS must be to make this crime *harder,* not *easier,* for identity thieves to commit.

Identity theft is growing at a truly alarming rate. According to the most recent figures from the Bureau of Justice Statistics, more than 17.6 million Americans – including 2.6 million seniors – fell victim to this terrible crime in 2014. Seniors are attractive targets for identity thieves because they are more likely to have life savings, own their own home, and have good credit. All of us on this Committee have heard heartbreaking stories from our constituents, especially seniors, who have been victimized by this crime. Identity theft

doesn't just rob its victims of their money and their credit, it robs them of their sense of security and peace of mind.

As we have heard in previous hearings, most recently our series on small business cybersecurity, too often small businesses are a target for this type of cybercrime because they often lack the resources to protect themselves. It has become clear that the IRS, like all agencies trusted with the American people's most sensitive personal information, needs to step up its game.

While the IRS may have taken a few limited steps in the right direction, then there are countless additional steps that must be taken to ensure taxpayer information is adequately protected. To be clear, this is **not** an issue of funding at the IRS. It is an issue of **priorities** at the IRS. If the IRS can pay out big bonuses to its employees – some of whom were implicated in the targeting of Americans for their political views - it should be able to find the money to protect people's data from identity thieves. If the IRS can pay for its employees to travel to union training events and prioritize the enforcement of ObamaCare over basic customer service, then there really is no excuse for failing to protect taxpayer information from thieves.

Our witness today is charged with periodically evaluating the IRS' efforts to safeguard taxpayers' personal information, including those of small businesses. It is my hope that he will shed light on the specific systems and procedures currently in place at the IRS and make recommendations for improvement going forward.

I am looking forward to hearing from Inspector General George. I now yield to our Ranking Member, Ms. Velázquez, for her opening statement.