PREPARED STATEMENT

of

Genie Barton
President
BBB Institute for Marketplace Trust

Hearing on
Robocall Scams

Before the
United States Senate Special Committee on Aging

Wednesday, October 4, 2017

Chairman Collins, Ranking Member Casey, Members of the Committee, thank you for giving me the opportunity to appear before you today.

My name is Genie Barton, and I serve as President of the BBB Institute for Marketplace Trust (BBBI).

I appreciate the opportunity to describe for the Committee BBBI's ongoing work to fight scams. In the United States, 50 billion dollars are lost to scams every year.[1] Data collected through our new, crowd-sourced BBB Scam Tracker tool has greatly enhanced our understanding of the nature of this intractable problem and how to combat it. In this testimony, I will summarize our recent work, including relevant insights from our research and reports, and provide data focused on scams that prey on seniors, including scams initiated by robocalls.

BBBI is the 501(c)3 educational arm of the Council of Better Business Bureaus, the national umbrella organization of the more than 100 local Better Business Bureaus serving communities across North America. BBBI partners with and leverages the reach of the BBB network. Every BBB in North America participates in Scam Tracker, reviewing and screening each consumer report before it is entered in the central data base, which is powered by BBBI. [2] BBBI then publishes the reports.

BBBI equips BBB staff with resources and training programs that help them to better serve their communities, particularly seniors. Grassroots senior educational programs have long been an important focus of BBB educational outreach, with scams being a major part of this outreach. Local BBB offices often have relationships with state agencies working to address the interests of seniors and relationships with senior centers in their communities. For example, the BBB located in Pittsburgh, Pennsylvania works through the Pennsylvania Department of Aging, and many of its over 90 presentations last year took place at senior community centers in its service area. BBBs power BBB Scam Tracker by reviewing each scam report, and they routinely field inquiries and share data with state and local law enforcement, especially Offices of State Attorneys General.

For more than 100 years, BBB has been working to build a trustworthy marketplace where consumers and responsible businesses can prosper. In the United States, 50 billion dollars are lost to scams every year.[3] There is, we believe, no greater threat to consumers and legitimate businesses than the fraud perpetrated by con artists.

---

[1] Martha Deevy and Michaela Beals, *The Scope of the Problem: An Overview of Fraud Prevalence Measurement*, Financial Fraud Research Center, 2013. http://longevity.stanford.edu/wp-content/uploads/2016/07/Scope-of-the-Problem-FINAL_corrected2.pdf at 28.

[2] The over 100 BBBs in North America vet the scam reports that originate in their service area, using both software and staff review to determine whether the consumer is reporting an event that a reasonable person would consider to be a scam or fraud. Only those reports are passed on to BBBI for publication in BBB Scam Tracker. Please note that we are not able to investigate and independently verify that an actual fraud has occurred, only that the *allegations* of fraud appear well-founded.

[3] Martha Deevy and Michaela Beals, *The Scope of the Problem: An Overview of Fraud Prevalence Measurement*, Financial Fraud Research Center, 2013. http://longevity.stanford.edu/wp-content/uploads/2016/07/Scope-of-the-Problem-FINAL_corrected2.pdf at 28.

It not only robs both consumers and legitimate businesses, but it does far more harm. It humiliates the individual scam victim. It damages the reputation of ethical businesses whose identities scammers assume. Finally, scams erode consumer trust and engagement in the marketplace.

BBB Scam Tracker

BBB Scam Tracker (www.bbb.org/scamtracker) gave BBB a crowd-sourced, digitally powered, 21st-century tactical weapon to fight the age old battle against fraud and deception. Launched throughout the U.S. and Canada in September 2015, BBB Scam Tracker is an interactive tool for consumers to report scams and fraud and warn others of malicious activity. Consumer reports capturing the scam in the consumer's own words are collected online and presented in a searchable online "heat map," showing consumers the number and types of scams reported in their communities. The tool provides a window on the scam landscape, enabling data-driven consumer alerts and tips based on current information. Reports are shared with the Federal Trade Commission for inclusion in its Consumer Sentinel database, with the National Cyber Forensics and Training Alliance, and with law enforcement agencies on request for investigative purposes.

Scam Tracker is well-positioned to operate as the pre-eminent consumer reporting tool about scams. Respondents to our 2016 survey of more than 2,000 individuals said they were more likely to turn to BBB to report scams than to anywhere else (including the police). A subsequent study by FINRA Foundation and Stanford Center for Longevity also found that BBB is the first organization the public thinks of to report a scam, providing independent verification.[4] To date, approximately 83,000[5] scam reports have been published, and the rate of reporting per day has increased by 54% from 2016 to the end of September this year.

BBB Scam Tracker's crowd-sourced approach taps the altruistic impulse that frequently motivates consumer reporting activity of scams and fraud. When consumers are asked what would drive them to report a scam, nearly 50% indicate that they would do so to help make sure it did not happen to someone else.[6] When the report is published, the consumer who has reported the scam often feels empowered by having taken action and less like a mere "victim". The consumer narratives drive home an important lesson—ordinary people like me get scammed. All of us are vulnerable. The impact of this reporting in warning others is amplified by our ability to connect reporters with individuals who are willing to be interviewed about their experiences.

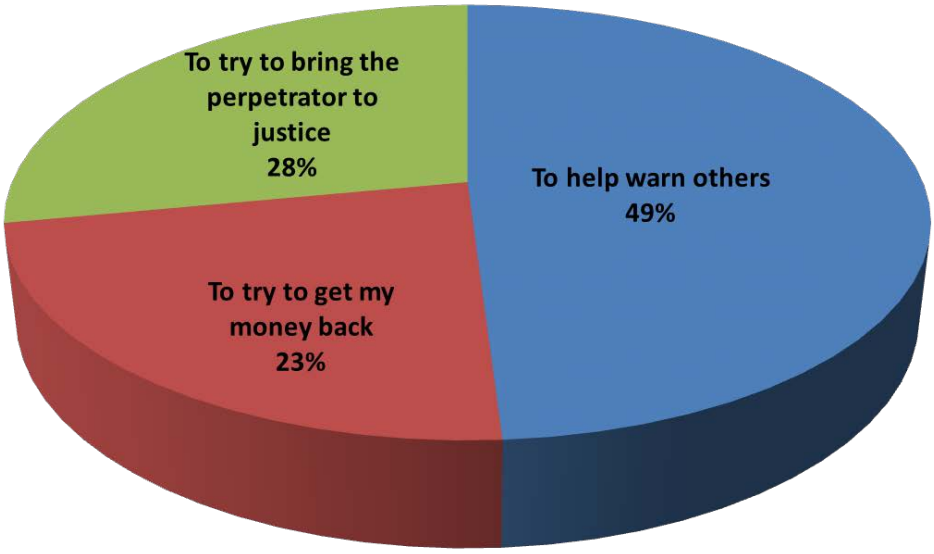
---

[4] *Findings From a Pilot Study to Measure Financial Fraud in the United States*, at 22, http://162.144.124.243/~longevl0/wp-content/uploads/2017/02/SCL-Fraud-Report-Feb-2017_Draft2.pdf.

[5] *See generally*, Better Business Bureau, *BBB Scam Tracker*, https://www.bbb.org/scamtracker/us (last visited Sep. 27, 2017).

[6] Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education at 5, https://www.bbb.org/globalassets/shared/media/truth-about-scams/bbb-scamprogram-whitepaper-08-digital-0630.pdf

Figure 1: Motives for Reporting a Scam



The data and stories we gather and share through BBB Scam Tracker also have given us the power to fight scams through new evidence-based research. This research gives us insight to better target and message our outreach to the general public and engages national and local media, boosting our effectiveness in raising public awareness. The reach and searchability of the Scam Tracker database also provides valuable assistance to law enforcement and regulators, and spurs academic researchers to add to our body of knowledge about scams.

Our 2016 study, *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*, shattered previous stereotypes about vulnerability to scams. In the study we demonstrated that that negative stereotypes around scam victimization predominate. When asked to describe a scam victim, consumers' responses were dominated by pejorative adjectives such as "naïve," "stupid," "gullible," "uninformed," and "old." We found that 83% percent of respondents believed that they were less at risk of being scammed than others.

Unfortunately, the belief that scams only happen to other people poses one of the biggest personal risks of all. Those who believe that it can't happen to them are less likely to heed warnings about scam activity and are not alert to the possibility that a seemingly legitimate phone call or email was actually from a scammer. One proof point is that the age group most likely to fall for a scam is actually millennials, a fact not widely recognized before this study. However, while on the whole seniors recognize their vulnerability and are therefore more cautious, when they are scammed they are most likely to suffer the largest financial loss.

While a number of studies have sought to understand the scope of the problem and the behavioral or psychological markers that distinguish scam victims, less has

been done to identify the knowledge and information that might be effective in preventing scam targets from becoming scam victims. With this in mind, our research was crafted to explore the contours of what a successful education and awareness campaign might look like. Nearly 80% respondents cited general knowledge of scam tactics and scam types as being most important in avoiding scams.[7] The insights about scam victimization that Scam Tracker provides are helping us to better focus educational efforts to more effectively alert consumers.

In speaking to millennials and seniors alike, we strive to counter negative stereotypes with stories of real people that collectively convey the message that this can happen to anyone. We are *all* at risk and, by talking about our experiences, we help protect others with essential information about scam tactics and types. We empower ourselves, and we begin to chip away at some of the shame and stigma surrounding this issue.

The statistical insights we have derived from Scam Tracker data are important, but the value of individual stories is immeasurable, as they make the problem real and convey the critical message that this can happen to anyone. These reports also help us to understand what messaging will be most likely to best alert consumers to common traps.

BBB Risk Index

In March of last year, BBBI release its first annual report of data gathered through BBB Scam Tracker, the *2016 BBB Scam Tracker Annual Risk Report*.[8] With this report we introduced the BBB Risk Index, a new, more nuanced conceptualization of risk. Prior to the introduction of the Index, attempts to compare scam types by relative risk, including by BBB, have generally consisted of simple rankings by frequency of exposure. This volume-based approach failed to acknowledge the multifaceted nature of scam risk. In fact, the risk posed to a given population by a particular scam type can best be understood by considering three dimensions: exposure, susceptibility, and monetary loss. By combining all three, as we have done with the BBB Risk Index, we are able to gain a far more meaningful measure of the relative risk of a given scam type. In our *Risk Report*, we applied the Index formula to various subgroups, including seniors, to identify the scams that present the greatest risk to each group.

To better understand the rationale for the Index, consider the broad spectrum of techniques employed across the scam landscape. On one end of the spectrum, a fraudster may employ a "wide net" approach. Robocalls, the subject of the hearing today, are an example of this technique. A scammer can inexpensively utilize robocalling technology to reach perhaps hundreds of thousands of individuals to find those few who would succumb to the ploy. While these scams reach a wide swath of the population, the susceptibility of those exposed is typically quite low.

---

[7] *Id* at 12.

[8] *2016 BBB Scam Tracker Annual Risk Report: A New Paradigm for Understanding Scam Risk* www.bbb.org/riskreport.

At the other end of the spectrum is the far more intensive "high-touch" approach, as is commonly seen with romance and investment scams. These scams reach fewer individuals, but those exposed are often more likely to be successfully conned. Monetary loss is a final critical element. A con that separates mere pennies from its victims may do tremendous overall harm if it impacts a large portion of the population, while a scheme with relatively few victims may be of even greater concern if median losses are extremely high. The Index captures these real-world elements by representing the intersection of exposure, susceptibility, and monetary loss.

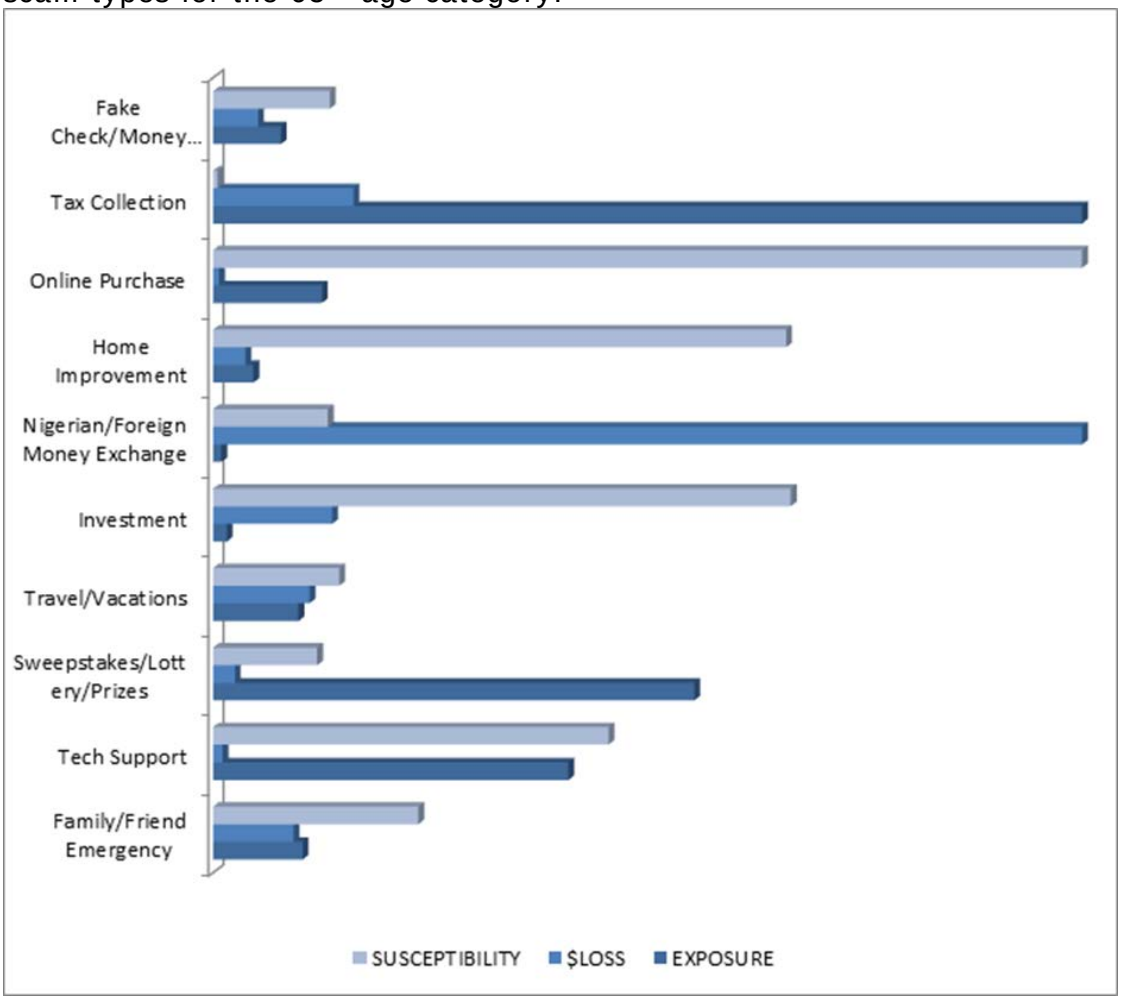
No law enforcement or regulatory agency has the resources to fight every scam. The Risk Index can help establish policy priorities and suggest resource allocation. The Risk Index can determine what are the greatest risks to a particular cohort of interest. In this testimony, we use the Risk Index to define the top 10 riskiest scams for seniors.

Approximately 16% of reports to BBB Scam Tracker are from individuals over the age of 65.[9] By applying the BBB Risk Index discussed earlier, we are able to identify the following scam types as being the top 10 most risky for this cohort.

1. Family/Friend emergency
2. Tech Support
3. Sweepstakes/Lottery/Prizes
4. Travel/Vacations
5. Investment
6. Nigerian/Foreign Money Exchange
7. Home Improvement
8. Online Purchase
9. Tax Collection
10. Fake Check/Money Order

[9] Data reported in this testimony is based on U.S. reports submitted to BBB Scam Tracker and published from the inception of Scam Tracker on February 13, 2015 through September 27, 2017, a period of approximately 20 months, except where otherwise indicated. These data updates result in statistics that differ from data reported in the *2016 BBB Scam Tracker Annual Risk Report*.

Figure 2 –Chart representing susceptibility, loss and exposure for top 10 risky scam types for the 65+ age category.



For seven out of these top ten scam types, the method of initial contact was a telephone call. In fact, 71% of *all* scams reported by seniors age 65+ began with a call. However, when we only look at reports that involved a monetary loss (i.e., where the target avoided the con), just 33% were initiated by telephone. This variance reflects the relatively low susceptibility levels common with telephone scams, particularly telephone scams that tend to be high-volume. For example, only 1 in 278 reports by seniors of the tax collection scam involved a dollar loss. Nonetheless, these scams are among the most risky to seniors due to high exposure levels and serious monetary losses.

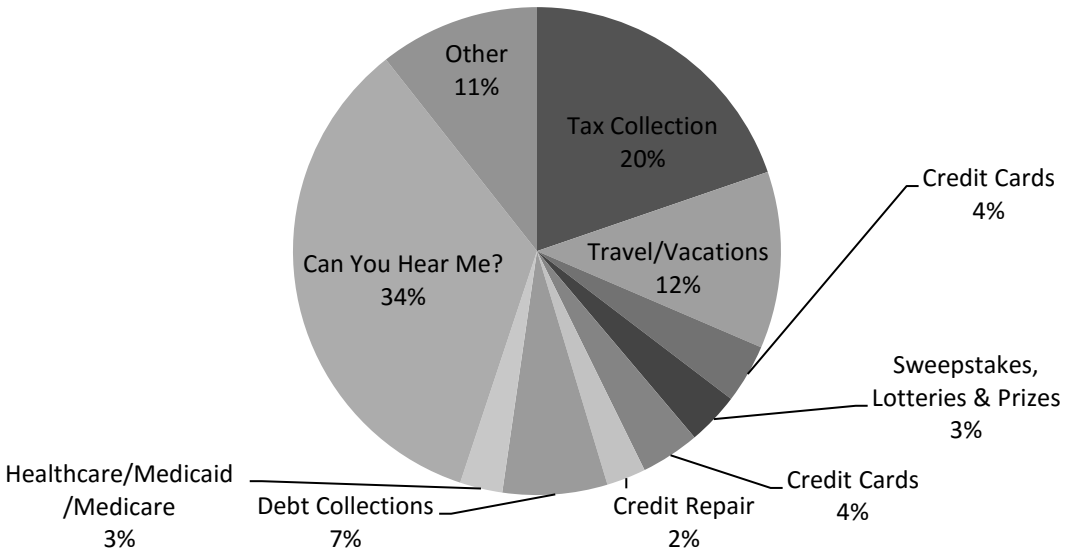
Our data show that when a senior loses money to a scam, the dollar loss is typically nearly 56% greater than losses incurred by younger individuals. The median reported loss by seniors is $390, while the median loss reported by those under the age of 65 is $250. The harm to retirees is further exacerbated because they are likely living on a fixed income.

Robocall Data

While we ask individuals reporting a scam to indicate if the scam was initiated by telephone, we do not currently ask if a robocall was involved. We are therefore unable to provide precise information on the percentage of all scams reported to us that were initiated by robocalls. We will consider revising this question to shed greater light on the impact of scams initiated by robocalls.

Fortunately, we do have the ability to search by keyword and have done so with respect to robocalls. The more than 400 mentions of the keyword "robocall" in consumer narratives about their experiences serve as a marker to help us understand which scams are most common among those perpetrated using this technology. The distribution of keyword "robocall" across scam types is represented in Figure 3.

Figure 3 – Scam type distribution of reports with keyword "robocall" during the period of January 1st 2016 to June 20th 2017.



There were no reports of the "family and friend emergency" scam that included the word "robocall," and tech support scams were grouped in the "other" category as just five of these reports included this keyword. These two common and high-risk telephone scams thus appear to be infrequently perpetrated using robocall technology.

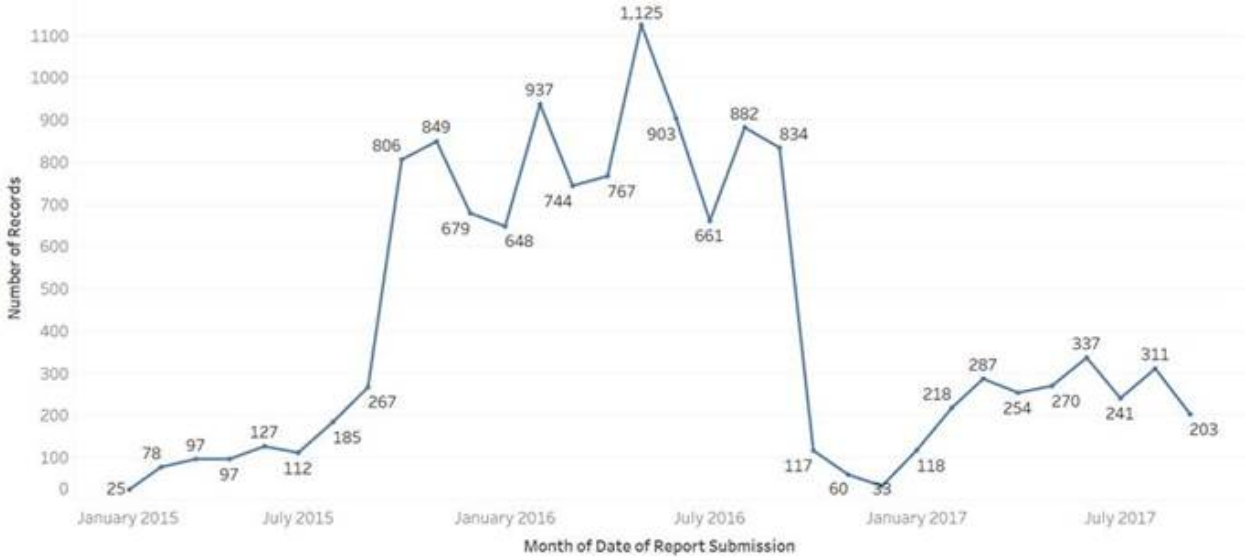
However, we caveat this conclusion based on the fact that a high number of scams are initiated by telephone and not all consumers will highlight the fact that some form of autodialer may have been used to initiate contact.

IRS Tax Collection Scam

Given that seniors are more vulnerable to the tax scam as compared to other demographics and tend to suffer greater financial losses, I would like to expand here on the information available to us on this scam type as gathered through BBB Scam Tracker reports.

In 2016, approximately 27% of all scams reported to us by seniors and 16% of scams across all age groups were classified as tax collection scams. The police raid on a call center in Mumbai, India in October 2016 resulted in an immediate 95% drop in reports of tax collection scams to BBB Scam Tracker, a decrease that continued through December of 2016, as shown in Figure 4. By January of 2017, reports of the tax scam were on the rise again, but much more slowly than in 2016. The steep drop in reports in fall 2016 is suggestive of a correlation. Today, our volume of tax scam reports has risen but is approximately 30% of the volume seen at the peak in 2016. While our data cannot explain why reports have not risen to 2016 highs, our ability to immediately detect these shifts shows the power and sensitivity of BBB Scam Tracker to take the pulse of the scam marketplace.

Figure 4: Evolution of Reports of Tax Collection Scams from January 2015 to September 2017.



As was set forth in Figure 3 above, we estimate that the IRS scam represents 20% of all robocall scams. While susceptibility levels are low, median losses are very high relative to other scam types. The median loss reported by seniors is more than $3,000. Payment is typically collected by directing victims to read the numbers from prepaid cards, often iTunes cards, or to wire funds. Scammers often provide specific instructions about retail locations to complete these transactions, and are known to direct consumers to move from one location to another to reduce the risk of intervention by agents of the wire transfer services.

The statistical data we are able to derive from BBB Scam Tracker yield valuable insights. In addition, consumer narratives are highly instructive and help us to

understand the way scammers are working, how consumers are "falling for" the scam, and what educational approaches might be helpful. The following is an account reported to BBB Scam Tracker by a senior in Indiana who lost $10,000:

"I received a phone call from a man claiming to be with IRS stating that I owed money. If I didn't pay they would send me to prison. He stated I would need to go to Walmart (4 different locations) to send money to them. I did wire money to them as requested. I figure that I sent approx. $10,000 total via wire transfer. I sent the money . . . I did this because I didn't want to go to prison. I thought they were honest people. I now know this was a scam."

BBB has found simple, unambiguous consumer fraud prevention messages to be the most effective. For years BBB had a simple message for consumers: the IRS will never call to demand immediate payment. However, in light of the fact that now that the IRS is using four private collection agencies (PCAs) to call consumers about outstanding debt, BBB has retooled our consumer fraud messaging to focus instead on pressure techniques and payment methods. We now emphasize that the IRS or its representatives will never ask you to pay over the telephone and that payments can be made in only one of two ways: Online at IRS.gov or by check or money order made out to the U.S. Treasury. We also make sure that consumers know that the IRS will never threaten them with arrest.[10]

Fraud prevention messages emphasizing that the IRS or its PCA representatives will never call you without first sending at least two letters are less helpful and may be problematic because individuals who receive these letters may also receive tax scam calls. Consumers who did not receive letters may assume that the letters simply got lost in the mail. We also know that scammers have learned to reference letters, even using the identifying codes for legitimate IRS notices, as we see in this recent report from a woman in New York who lost nearly $11,000:

"'Agent Teresa Moss' and 'Agent Richard Watson' called me and told me I had a warrant for my arrest for tax evasion . . . . they were the IRS and had sent me letters (which I never received). They asked me if I lived at my address (I confirmed that they had the correct address), but I told them I was certain I never received these notices (they called them the 'CP 200 notice,' and the 'CP 11A notice') . . . . throughout the day they instructed which stores around my home I could visit to purchase $50 and $100 iTunes gift cards. I was then to immediately scratch off the sticker on the back and recite the serial code to them. I was to buy only a few at a time and not attract suspicion within the various stores . . . For eight hours I walked around and purchased these gift cards."

The threat of arrest is a common intimidation tactic and is characteristic of many of the IRS scam reports where consumers suffered a monetary loss. Therefore anti-fraud messaging that states that the IRS or PCAs acting on behalf of the IRS will never threaten you with arrest may also be useful and may help prevent consumers from getting rattled and panicking.

[10] BBB runs scam alerts on the Scam Tracker website and also provides consumer tips on scams, including the IRS scam. *See, e.g.* BBB tips explaining the tax scam in the U.S. and Canada at https://www.bbb.org/taxscam/.

"Can you hear me?" Scam

Beginning in early 2017, BBB began to receive large numbers of reports involving interactive robocalls where consumers are asked "Can you hear me?" or some variant apparently intended to solicit a "yes" response. A staggering one third of all published reports to BBB Scam Tracker this year to June 30th, 2017 can be classified as "Can you hear me?" calls.[11] As shown in Figure 3, 34% of all reports with keyword "robocall" are "Can you hear me?" calls. Often, these calls terminate immediately following a response. In other instances, the calls continue with additional recorded content and questions. Some are transferred to a live operator. The purported intent of these calls varies, and includes free vacations, sweepstakes, and government grants. Interestingly, only a tiny fraction of these reports (fewer than 1 in 1,000 reports) relate to tax collection. We believe the volume of reports is, at least in part, attributable to significant media coverage around this problem, but it also suggests a concerning trend toward more sophisticated uses of interactive robocall technology by con artists.

The example of a report below shows an individual who reported a $199 dollar loss due to a Robocall scam scenario.

"[T]hey call you saying that you have been approved for a loan. they are going to ask if you are able to hear them, say no...do not say yes. they more then [sic] likely have all your information already. they [sic] will go through all that with you. and then they tell you that they are not able to use your accounts due to fees, and say that they can western union the money to you as long as you pay the fees first. if [sic] you decided to cancel your decision, they will say that you now owe them $199 cancellation fees. and they will take it directly from your account"

The example of a report below shows an individual who encountered a robocall scam scenario but did not incur a financial loss.

"I received a call asking if I wanted to follow up on an inquiry for employment. Seeing as I've been applying for jobs, and honestly a bit desperate for one being a college student, I immediately fell into "interview mode" and said "yes" only for them to hang up. Nothing has actually happened yet, however with the sheer amount of scammers going around I felt like others should know about this method in case something does happen. I already had anxiety about answering the phone for numbers I'm not familiar with, and this is only making it much worse."

Of the nearly 10,000 published "Can you hear me?" reports, fewer than 20 involve a reported dollar loss, and those losses cannot be definitively connected to a "yes" response. We remain uncertain as to precisely what is the endgame of these scams. Cramming may be one possible outcome, but it is also possible that the "Can you hear me?" question is intended simply to confirm a live person has answered. The information we have on the volume and substance of these calls suggests an intent

[11] "Can you hear me?" is not one of the 30 scam types used in BBB Scam Tracker. The vast majority of these reports are classified as "phishing" or "travel/vacations." For purposes of Figure 3, we have reclassified reports as needed to create a "Can you hear me?" category.

to perpetrate a scam, but there are a large number where the caller simply disconnects, perhaps suggestive of a nasty, annoying prank.

Conclusion

In conclusion, we stand ready to assist this Special Committee, other congressional committees, the FTC, the IRS, the FBI, and any federal, state, or local agency with efforts to protect consumers from scams. As we have learned through our data collection and through our research, everyone is at risk. Everyone is vulnerable. We believe that government, media, consumer stakeholder groups, industry associations, and individual businesses both large and small, all have a role to play to fight back effectively against scams. BBB offers tools to help empower consumers to identify the common tactics and to learn to recognize the “red flags” that indicate a scam. We welcome the opportunity to share our data, our messaging, and our outreach capabilities to help put a halt to this immense problem.

Thank you very much for inviting me to be here today, and I would welcome the opportunity to answer any questions you may have.