



# GOVERNMENT IMPOSTOR SCAMS

---

Reports decrease, scammers pivot for new opportunities, BBB study reveals

ISSUED: JULY 2020

# It starts with a “government” phone call...

Suppose you get an unexpected telephone call from a government agency telling you that a police officer will be there shortly to arrest you. Most people would be shocked and afraid. The caller seems legitimate, providing badge numbers and perhaps even personal information about you. The caller ID displays the name of a real government agency. Here's the catch: the caller claims jail time can be avoided if you pay a fine by immediately going to a store, purchasing gift cards, and reporting the code numbers to them.

# 44%

of Americans have encountered a government impostor scam

Over the last several years, the public has been under assault by scammers impersonating a multitude of government agencies. Research by Better Business Bureau (BBB) found the Social Security Administration, Service Canada, the Internal Revenue Service and the Canada Revenue Agency are among the most widely impersonated agencies.

However, during the COVID-19 pandemic and after the passage of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), even the Centers for Disease Control (CDC) and United States Treasury Department's names have been used by scammers to manipulate and steal from unwitting consumers.

In other scenarios, scammers threaten arrest for missing jury duty, impersonate immigration officials and threaten to deport people, or offer free money in the form of government grants.

**A recent AARP survey found that 44% of Americans over the age of 18 had been exposed to these types of scams. Also, 77% of those surveyed were at least somewhat familiar with government impostor scams. BBB estimates victims have collectively lost hundreds of millions of dollars.**



Most of these calls appear to originate in India, and law enforcement in the U.S. and Canada have aggressively prosecuted people here that launder the money from victims. Although law enforcement in India has made efforts to close down some of the originating call centers, actual prosecutions or extraditions have been rare.

In a Justice Department Journal of Federal Law and Practice [article](#) about efforts to fight telemarketing fraud coming from India, the department official who authored the piece said: “Little evidence exists to suggest that the Indian government will successfully prosecute and impose significant sentences on the perpetrators of these call center scams operating within Ahmedabad and elsewhere within India.”




There has been a dramatic drop in complaints in the U.S. about these scams so far in 2020. Because such calls are made using Voice over Internet (VoIP) systems, they have to travel through a “gateway carrier” to enter the domestic phone system and reach victims. U.S. law enforcement has been taking action against these gateway carriers, and this tactic has resulted in a

## How the scam works

You get a call.

-  Your caller ID might show it's the IRS calling.
-  The caller might give a badge number and know the last four digits of your Social Security number.

You are told:

-  “You owe money.”
-  “You better pay now or you'll be arrested.”
-  “Put money on a prepaid debit card or wire it to us.”

If you pay...

-  You find out it wasn't the IRS. It was a scam. → **The money is gone.**



(Federal Trade Commission)

sharp drop in automated recorded “robocalls” from outside the U.S. The same enforcement actions also took aim at caller ID spoofing.

Though scam calls have been reduced in the U.S., they have not been eliminated. Clever scammers will look for ways to evade these controls and adapt to law enforcement's strides in preventing fraud. For example, in a recent development during the COVID-19 pandemic, the Treasury Inspector General for Tax Administration (TIGTA) says it has received over 1,700 complaints about calls supposedly from “IRS agents” who claim they can speed up stimulus payments under the CARES Act passed during the pandemic. Scammers get personal information from victims and use it to have government payments redirected to accounts they control.

This BBB study examines the size of the government impostor problem, identifies who is affected, examines the types of fraudulent claims made to victims of these scams, explains the elements needed to operate the scams, and looks at law enforcement efforts to identify and apprehend the perpetrators.



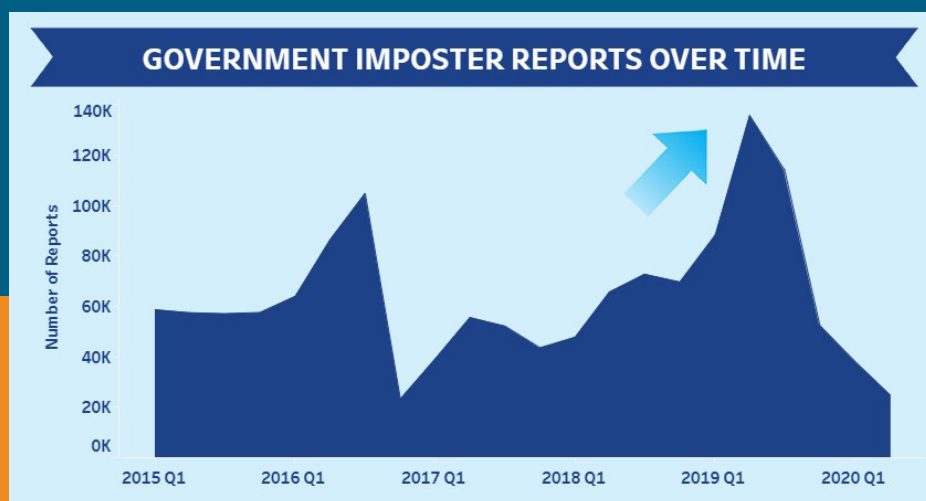
# HOW COMMON IS GOVERNMENT IMPOSTOR FRAUD?

Government impostor scams produce many complaints to BBB, the Federal Trade Commission (FTC) and the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3).

In 2019, BBB reports about scammers impersonating tax officials dropped sharply while reports about Social Security Administration (SSA) impersonators quadrupled in the U.S. Complaints about calls from Service Canada, however, have increased this year.

## Total government impostor complaints

YEAR	FTC	IC3	BBB SCAM TRACKER
2017	188,879	9,149	3,207
2018	254,626	10,978	3,862
2019	391,892	13,873	2,863
2020 (through 6/30)	62,970	664	



## IRS impostor complaints to BBB Scam Tracker

YEAR	COMPLAINTS
2017	2,105
2018	2,300
2019	251
2020 (through 6/30)	31

## SSA impostor complaints to BBB Scam Tracker

YEAR	COMPLAINTS
2017	134
2018	479
2019	1,963
2020 (through 6/30)	515

## Canada Revenue Agency impostor complaints

YEAR	COMPLAINTS
2018	22,434
2019	3,245
2020 (through 5/14)	609

## Service Canada impostor complaints

YEAR	COMPLAINTS
2018	not available
2019	4,181
2020 (through 5/14)	3,875

## Internet Crime Complaint Center

YEAR	DOLLAR AMOUNT
2017	\$12.47 million
2018	\$64.21 million
2019	\$124.29 million

## Canadian Anti-Fraud Centre (CAFC)

YEAR	CANADA REVENUE AGENCY	SERVICE CANADA
2018	\$6.412 million	not available
2019	\$1.49 million	\$1.29 million
2020	\$303,609 (through 5/14)	\$1.228 million (through 6/30)

# HOW MUCH MONEY IS LOST TO GOVERNMENT IMPOSTOR FRAUD?

The amount of money lost to this fraud is staggering. In July 2019, the [FTC estimated](#) victims lost \$450 million from 2014 until that time. This chart shows the losses reported to IC3 have quickly grown. (The FTC does not release annual loss numbers in its yearly reports.)

### How many of those receiving a government impostor call lose money?

The [FTC estimates](#) that about 6% of those receiving these calls lose money. As noted, however, even if most people do not respond to these calls, it is still a highly profitable endeavor for the scammers.

### How are people contacted about government impostor scams?

The [FTC estimates](#) that contact is initiated by telephone 96% of the time. Some people also get emails, text messages or fake letters.

### What is the average age of victims of impostor scams?

People ages 20-59 were more likely to lose money to these scams than those 60 years or older, but older victims were more likely to lose larger amounts of money, according to [FTC estimates](#). AARP found that younger victims ages 18-49 are more likely to have health/emotional consequences from this scam; 25% of victims in this age group were found to experience these, versus 12% of older victims.

### What are the average losses to these scams?

The amount of money lost can vary dramatically, from just a couple of hundred dollars to very large amounts. The [FTC found](#) that the median amount lost was \$960. However, median losses for those over 60 were \$2,700.

### How do victims pay?

Victims pay through gift cards and reloadable cards 58% of the time, according to [FTC research](#). Another 13% paid by wire transfer, either a bank-to-bank transfer or through Western Union or MoneyGram. The most recent complaints show that the majority of victims pay by gift card. Scammers do not need the card itself. They can access the money loaded on the cards if victims simply provide the scratch-off numbers on the back. Because many scammers also try to obtain bank account information, it is likely that money is also being stolen from victims' accounts. In addition, many victims are being asked to send cash by mail or Federal Express.





# MOST COMMON TYPES *of* GOVERNMENT IMPOSTOR SCAMS



**At present, the bulk of complaints are about calls supposedly from the U.S. Social Security Administration (SSA) or, in Canada, its counterpart Service Canada.**

These scams often -- though not always -- begin with a robocall which, if not answered, leaves a voicemail message instructing the victim to call back. Most threaten an imminent arrest or legal action if the victim does not return the call. The number displayed on the caller ID is not the actual source of the call. In the course of these scams, they often also impersonate the FBI, Drug Enforcement Administration (DEA), and other enforcement agencies.

## Social Security/Service Canada impersonators

Several different [tactics](#) are employed by these [scammers](#). Most involve robocalls or direct phone calls, but SSA has [recently warned](#) that scammers have supplemented their efforts by sending emails to victims with attachments that look like official correspondence from SSA or the SSA Inspector General (SSA IG). These fake documents direct victims to call a specified "officer."

Both the [SSA IG](#) and [Service Canada](#) have issued warnings to the public about impostor scams. In particular, [the FTC reminds the public](#) that Social Security numbers are never "suspended." BBB also has issued warnings about [Social Security impostors](#).

**Increase a benefit:** Some callers tell victims that they are eligible for increased Social Security benefits, typically claiming that it's for a cost of living increase. The caller requests bank account details so that the money can be deposited into the victim's account. Once the scammers have the victim's bank account information, they are able to steal money from those accounts. This version of the scam only works for victims eligible for benefits.

**Restore Social Security number:** Other callers claim that the victim's number has been suspended. The victim is asked for a payment to "restore" the number. In some variations, the scammers need details about the victim's Social Security account. If that information is provided, the scammer can apply for benefits in a victim's name or have the benefits redirected to accounts the scammer controls.

### Appendix C



#### SOCIAL SECURITY

##### MEMORANDUM

Date: September 30, 2019

Refer To: Case ID: DC-7054

To: [REDACTED]

From: Social Security Administration (SSA)

Subject: Re-issuing social security number for the cause of identity theft.

The Office of Inspector General (OIG) & the Social Security Administration hereby acknowledge to provide a replacement social security number for [REDACTED] entitled to [REDACTED] after the fulfillment of the ADR procedure.

The SSA confirms the change in social security number after the confirmation from DEA about the ADR fulfillment, for further procedure information please contact the assigned officer for further information.

This letter is a subject to information just intended for [REDACTED], not for use in legal proceedings.

S. [REDACTED]  
Acting Deputy Chief of Investigation

##### MEMORANDUM

Date: 30 September 2019

To: [REDACTED]

From: Inspector General

Subject: (OIG)'s assurance policy for the secured assets of case ID: DC7054.

The Office of Inspector General (OIG) states in regards to case ID: DC7054 to [REDACTED] for the reimbursement of the assets surrendered for the security locker to the attorney general would be provided in the form of cashier's check issued in accordance by the U.S. Treasury Department.

Taxes payed during the ADR procedures would be payed as a reimbursement by the Office of Inspector general in accordance with the U.S. Treasury Department after the completion of Alternate Dispute Resolution (ADR).

In regards with further case details please contact the allotted Officer [REDACTED] with the case id and the details of the case on [REDACTED]

Gail S. Ennis  
Inspector General

Investigation report [REDACTED] (4-08-DC7054) (C)

# MOST COMMON TYPES *of* GOVERNMENT IMPOSTOR SCAMS

(CONTINUED)

## Social Security or Social Insurance

**Number used in a crime:** Perhaps the most common Social Security-related scam involves threat of arrest. Scammers call directly or leave voicemail messages telling victims that if they do not call back, they will be arrested right away. The FTC has posted one of these [Social Security scam recordings](#).

Callers pretend to be law enforcement, such as the FBI, Royal Canadian Mounted Police (RCMP) or DEA. They tell victims a car was found abandoned with drugs and blood in it, often in El Paso, Texas, and that the car was rented using the victim's Social Security number. When

people deny involvement, the "officer" then says they must be an identity theft victim and money needs to be moved out of their bank accounts temporarily because

- 1) the ID thieves may steal it or
- 2) the government is freezing it because of criminal charges.

Thus, they have victims withdraw money from their bank accounts, buy gift cards, and read the numbers over the phone to the "agent." These scammers claim they will visit the victim at their home in a few days, return their money, and provide them with a new Social Security number.

**T**his scam successfully defrauded a Chicago college basketball coach named **London**. After a team workout in June 2019, he listened to a voicemail message from the Social Security Administration advising him that his identity had been used in Texas and asking him to call back.

He returned the call and spoke to a man who claimed to be with Social Security. The caller said someone using London's identity had been involved in a cocaine deal in Texas and that there was a warrant out for his arrest. The caller already knew a great deal of information about London, including his parent's names and email addresses. London said he was scared at the time.

The caller then transferred London to "Officer Hayden Smith" of the DEA, who provided his badge number. Smith said there was an open investigation on London and asked for his cooperation. He said if London didn't cooperate, a warrant would be issued for his arrest and the crime would

be made public. Smith stressed that if London hung up the phone, he would be immediately arrested.

Smith said London's bank account was frozen. In order to move the funds out of his personal account and into a "safety account," London would have to buy Target gift cards, which the police would turn over to the U.S. Treasury to place into an account where his money would be safe.



London was told to buy Target gift cards in the same amount as his bank account balance. He withdrew all the money in both his checking and savings accounts. Smith

A BBB office in Wisconsin returned one of these calls and played along until asked for bank account information. They have [posted the call on YouTube](#).



directed London to drive to five different Target stores to buy more than \$28,000 in gift cards while he stayed on the phone. After the final purchase, London read the numbers from the cards to Smith in the parking lot. Before reading them all, London used his phone to look up "fake call scammers" and found an FTC warning describing this type of call. He knew then that he was scammed, and he said, "You're scamming me. I'm hanging up." The agent then said, "You don't want to do that, this is for the police." The scammers kept calling back, and London's mom got on the phone and cursed them for their actions.

London knew the president of BBB of Central Ohio and called him for advice. He filed reports with BBB, the police and Target. He was able to recoup \$2,000 because he hadn't provided all of the gift card numbers to the scammers, but the rest of the money was gone.



# MOST COMMON TYPES of GOVERNMENT IMPOSTOR SCAMS

(CONTINUED)

**L**ina is a St. Louis teacher who had a similar experience in June 2019 when she received two robocalls from “Social Security” on the same day. She knew a bit about scam calls pretending to be the IRS and tech support scams, and she knew from her work that Social Security does not call people by phone, so she was skeptical.

The first call, which she did not return, was a robotic-sounding voicemail message that claimed her Social Security number had been compromised and instructed her to call the number that appeared on her caller ID. She did not respond. Lina says that this recording was the same as the one captured on [nomorobo.com's website](http://nomorobo.com's website).

Later that day, a second robocall recording -- from a cellphone number [registered with a company in India](#) -- prompted her to “press one” to talk to a live person. The man who answered told Lina her Social Security number had been compromised and asked for her full name and the last four digits of her Social Security number.

Lina made up a fake name and gave the man four random numbers instead of her real Social Security information. The man told Lina he saw her case and that her Social Security number had been used in El Paso, Texas and had been linked to drug trafficking and money laundering. He asked her if she had a bank account with Bank of America, Wells Fargo or Chase or if she had

shared her information with anyone. She told him no.

He then provided her with a case number and a warrant identification number.

The man told Lina she needed to pay \$8,900 and an additional \$1,000. The reason for these amounts was unclear. He asked if she had left her purse unattended, apparently suggesting she might be a victim of identity theft. Lina said she would never risk losing her information because there are people out there taking advantage and scamming them. At that point, the caller recognized Lina's suspicion and hung up on her. Lina reported the incident to BBB to help prevent others from being scammed.



## Internal Revenue Service/Canada Revenue Agency impostors

Although the exact nature of these calls varies, there are several clear points of similarity. The caller pretends to be a federal agent and claims the victim is about to be arrested for unpaid taxes or for tax fraud, often pretending that officers will be there within an hour or two to arrest them. But the victim can avoid this if they pay a fine, or the unpaid taxes, immediately. Victims are told to go to a local store to buy gift cards and then provide the caller with the numbers on the back of each card. Often the caller stays on the telephone with the victim throughout this process, sometimes for hours.

The [IRS](#) and [TIGTA](#) have issued warnings about this fraud, and TIGTA has published a [video](#) as well. The Canada Revenue Agency also has [issued public advice about tax scams](#), and BBB has issued [alerts](#).

Mr BOB [REDACTED]  
Before I start off I need to introduce myself as Ben McCoy, Special Agent in Charge of the Office of Inspector General for the U.S. Department of Tax Administration and IRS Tax Evasion cell-Texas Region. This line has been recorded for Scrutiny and surveillance purpose.  
You have a right to remain silent for next 2 minutes and you will have your right to speak after I complete.

Now Mr John [REDACTED] Your case id -- 7008974/2011case is being jointly investigated by agents with IRS and U.S. Treasury Inspector General for Tax Administration (TIGTA).

Your case id is registered with charges of Felony and Treason for :-

1. **Tax fraud and money laundering**—which carries a maximum sentence of 10 years in prison and a fine of up to \$100,000 with your Deportation back to your country imminent and on the cards with a water tight case against you with the Board of Deportation(B.O.D)
- 2 - **Unreported personal income and Tax Evasion and defaults on tax-** on American Soil Its an act of Treason and Felony , For not paying sufficient taxes and unaccounted personal income.  
**Now if charges are pressed:-**

A.ARRREST and DEPORTATION is imminent- In the next one hour Our team of Special Division of Asset Recovery would be at your doorstep which is responsible for the collections of federal debts and the forfeiture of assets related to Tax Evasion AND would be co-joined by the Financial Litigation Unit, responsible for the collection of civil debts DUE to the United States Government .And we would do it in an aggressive, efficient and effective manner.

SETTLEMENT-NO Leniency can be expected from us as we consider it as aggravated felonies" grounds for removal (deportation). Under immigration law, but YES we we have one aim that is to ensure that Taxes that you have evaded for these years go back to the IRS without Fail.

(If Customer is on his Knees after the Threats)-then go for the KILL(closing)

So MR..... how do you intend to do a Foreclosure and Pay up your impending Taxes ???...

You Can Apply for an Offer in Compromise (OIC)

*A sample script from an IRA impostor.*



# MOST COMMON TYPES *of* GOVERNMENT IMPOSTOR SCAMS

(CONTINUED)



## COVID-19

Scammers pay close attention to current events in order to further their schemes, and there have been numerous efforts to exploit the pandemic.

- TIGTA reports that callers have impersonated the IRS, claiming to expedite benefits under the CARES Act.
- The Centers for Disease Control and Prevention (CDC) [warns of scam calls displaying the CDC's phone number in caller ID](#). Some of these calls request donations. Emails or text messages may contain malicious programs that are downloaded if the recipient clicks on a link. IC3 has issued a [similar warning about fake CDC emails](#).
- [BBB warns](#) of texts, emails, or social media notices claiming to be from contact tracers, informing the recipient that they may have come in contact with someone who has tested positive to the virus. These may contain malicious attachments or seek personal information for use in other scams. The contact tracing scam has been [noted](#) as a particular problem in the UK.
- Financial Crimes Enforcement Network (FinCEN) recently issued an alert to U.S. financial institutions urging them to be alert to [government impostor and money mule scams that are related to COVID-19](#).

## Jury duty

In these [scams](#), callers tell victims that they have failed to report for jury duty, have ignored warnings about this issue, and are to be arrested within hours. Often these calls actually display the caller ID of the U.S. Marshals' office or the local sheriff's department. The victim is told that they can avoid arrest if they pay a fine and purchase gift cards. [BBB](#), the [U.S. Marshals Service](#), and the [U.S. Federal Courts](#) are only a few of the groups that have warned of this scam.

## Customs and immigration

This scam targets immigrants living in the United States or Canada. Victims are told there is an irregularity in their passport or immigration papers, and that they will be deported from the U.S. in days. Victims are instructed to buy gift cards to pay a fine. This scam also includes calls purporting to come from the U.S. Consulate in another country. They employ the same tactics to get money from victims. [U.S.](#) and [Canadian](#) governments have warned of this scam.

**D**anny received a call in 2018 from a man identifying himself as Captain Rolland from the local Wichita County (Texas) Sheriff's Department, telling him a warrant had been issued for his arrest as the result of failing to appear for scheduled jury duty. Danny was told he needed to pay a fine of \$9,500 by buying Green Dot MoneyPak "vouchers" at Office Depot. He was told he should buy the vouchers, provide the numbers to the caller, and go to the sheriff's department to explain his innocence. After that, the caller said, Danny's money would be refunded and all charges would be removed from his record.

When Danny asked if this was a scam, he was invited to do an internet search of the number on his caller ID. Danny did so, and the number did belong to the local sheriff's department. He said the callers were extremely polished and convincing. They kept him on the phone for over an hour before he asked his wife to call the local sheriff's office. She did, and they told her it was a scam. Danny then told the scammers he had the real sheriff's office on the other line, and they immediately hung up on him. He filed a complaint with BBB to help prevent others from falling for this scam. Not long after this event, the sheriff's office [issued an alert](#).



# MOST COMMON TYPES *of* GOVERNMENT IMPOSTOR SCAMS

(CONTINUED)

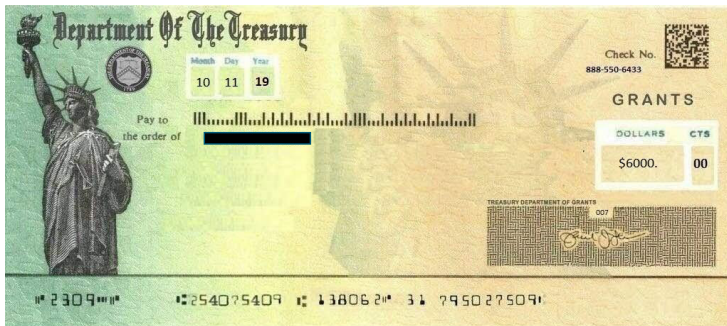
## Government grants

Victims receive calls stating the government is providing grants that don't need to be repaid. However, [scammers](#) tell victims fees are needed before the grant money can be delivered. The [FTC](#) and [BBB](#) have issued warnings about this scam.

Many of the grant scams locate victims on social media, where scammers send messages looking like they are from a Facebook friend that claims the “friend” recently was awarded a free grant worth thousands of dollars. The message urges the targeted victims to reach out to an agent by phone or text so they, too, can get a grant. Scammers then demand fees to get the grant, which is never delivered.

## Other types of government impersonation

There are other types of scams that rely on the authority of the government to get money or information from victims, and inventive scammers are likely to try new approaches. For example, lottery scammers calling from Costa Rica have impersonated actual people at the FTC and other agencies in lottery scams (including the author of this study). Others impersonate Medicare in efforts to file bogus claims for durable medical equipment like back braces.



**S**ylvie's case is typical of a grant scam. She lives in San Mateo, California, and works as a security guard. In October 2019, she received a voicemail message saying she had been randomly selected to receive a government grant of \$11,300. She confirms that it was [the same voicemail message posted at nomorobo.com](#).

She returned the call and talked to “Irene Johnson,” and Sylvie thought it sounded like she was talking to a call center in India. Irene connected her to another representative who asked her questions about the purpose of the grant, suggesting she respond that it was for education. Sylvie planned to use the money to help her son and daughter.

Irene told Sylvie there was a \$500 application fee, and told her to go to a store and buy a \$500 eBay gift card and call her back. Sylvie did as asked, returning the call, taking a photo of the pictures on the back of the card and sending that back as a text message.

Sylvie then got a call from “Adam Hunter,” who said he was with the Federal Reserve Bank and that they had two government checks for Sylvie for her grant money. But he told her she needed to buy another eBay gift card to cover “check processing fees.” She did, texting the photos to Hunter. Hunter then texted her photos of her government grant checks.

Hunter then had Sylvie buy additional gift cards to cover “delivery fees,” “tracking number fees,” and “California state taxes.” She spent \$2,000 on gift cards she provided to Hunter. Hunter promised all of this money, except the application fee, would be refunded to her, but it never was.

Hunter promised to have her grant checks delivered to her in person, but they never appeared. The money Sylvie sent was intended for her rent, car insurance, food and gas. She complained to eBay and her bank, but could not get any money out. Sylvie called BBB to file a complaint.

Sylvie called Irene and Adam to complain about being scammed, hoping to tie them up so they couldn't scam other people. They were rude, showed no empathy and told her she wouldn't get her money back.

**V**ictoria, an assistant manager at a Kwik Stop in Nebraska, had a similar experience. In December 2018, Victoria got an email purporting to be from the Federal Reserve Bank of New York. It said she was selected from a group of 1,500 people to receive a \$9,000 grant. She called the number provided and spoke to a man named Bill, who she said spoke with a thick accent and told her he'd moved to the U.S. from the Middle East. He told Victoria that to receive her grant, she had to pay a \$200 fee. Bill told Victoria that \$9,000 grant money would be directly deposited into her bank

account. He also told her she had to pay the fee or she would be arrested. Victoria was frightened and provided her bank account information. She had two small children at home and did not want to go to jail.

Bill instructed her to drive to a local Walmart to buy a Green Dot MoneyPak. He stayed on the phone with her while she did this. He had her scratch off the number on the back of the card, take a photo of the numbers, and text it to him.

After she had paid the money, Bill told her she needed to pay another \$150, promising it would

be refunded to her later. Victoria did not have enough money. Bill told her to go to the bank, and he would stay on the phone. She explained the situation to a bank manager, who told her it was a fraud, and that this was the second time that week someone had come in with this type of scam. The bank manager put the scammer on the speaker phone and asked a few questions. The scammer got angry and cursed at them, then hung up. Victoria never received the supposed grant.

# Red Flags

## How to identify impostor scams

How can you spot and avoid someone impersonating a government agency?

- **The IRS generally first contacts people by mail** -- not by phone -- about unpaid taxes.
  - Never provide your bank account or other personal information to anyone who calls you.
- **Don't pay by gift card.** The IRS and other government agencies will not insist on payment using an iTunes card, gift card, prepaid debit card, money order, bitcoin or by sending cash.
- **The IRS will never request personal or financial information by email, text, or any social media.** Don't click on links in emails or text messages.
- **Social Security numbers are never "suspended."**
- **Caller ID cannot be trusted** to confirm that the source of the call is a government agency. Look up the phone number for the real agency and call to see if they are really trying to contact you -- and why.
- **The Social Security Administration will never threaten to arrest you** because of an identity theft problem.

# KEY ELEMENTS OF GOVERNMENT IMPOSTOR SCAMS

## How do scammers know who to call? Lead lists.

Scammers buy lead lists of names, phone numbers, and other information about potential victims. This is not necessarily illegal, since there are legitimate uses for such leads. A quick internet search for "leads" shows hundreds, if not thousands, of sources that sell them. Sensitive personal information that is procured in data breaches is also sold in underground forums such as the dark web.

Many impostor victims report that the caller already had a great deal of personal information about them, sometimes including their Social Security numbers, which enhanced their credibility. In many cases, victims are asked to "confirm" personal information, suggesting the caller already has it. In reality, though, this may simply be an attempt to trick people into disclosing this information.



## VoIP calls and robocalls are popular with scammers.

Recently there have been strong law enforcement efforts to stem the flood of calls from India and elsewhere, particularly by targeting those who make the calls possible.

Scammers place calls to victims through a VoIP system, meaning they make the calls over a broadband internet connection rather than over a traditional phone. If the call is sent from outside the U.S., these calls must go through a "gateway carrier" before distribution to the major phone company systems and then to phones. This applies to both direct calls as well as robocalls. Most of these calls have codes that disguise the actual caller ID information and trick the system into displaying almost any originating number the scammers desire. By using this "spoofing" process, government impostor calls can show

the phone number of a real government agency. Finally, the telephone number needs to appear to be a U.S. telephone number for U.S. consumers to call back, or for when victims "press 1" to talk to a live operator. Many gateway carriers have provided scammers with all of these services.

Recently there have been efforts to combat VoIP calls, including robocalls. In 2019, the FTC sued Canada-based VoIP service provider [Globex](#) and [James Christiano](#) for transmitting robocalls into the United States. In December 2019, the U.S. adopted the [TRACED Act](#), which encourages the use of technology to combat robocalls and caller ID spoofing.

With help from the telecom industry, the FTC has been sending warning letters to gateway carriers in the U.S. alerting them that they can be legally liable for

assisting and facilitating fraud. The [FTC sent 19](#) such letters to U.S. VoIP providers in January 2020, [another nine](#) in March, and [two more in April](#) that came jointly from the FTC and the Federal Communications Commission (FCC). Since then, there has been a [reduction in the volume](#) of robocall complaints that the FTC receives.

The Justice Department filed [two cases](#) in January 2020 against gateway carriers that they alleged handled hundreds of millions of calls from India, many of them robocalls involving government impostors. Cases against [Tollfree Deals](#) and [Global Voicecom](#), Inc. allege similar facts. Both companies not only allowed robocalls into the U.S., but also were involved in spoofing caller IDs and in providing phone numbers for victims to call back that appeared to be domestic.



# KEY ELEMENTS *of* GOVERNMENT IMPOSTOR SCAMS

(CONTINUED)



In the Tollfree Deals case, the complaint alleges that, over a 23-day period in May and June 2019, the company transmitted 720 million calls into the U.S., including 143 million calls from one India-based operation alone. The callers claimed to be from Social Security, the IRS, and U.S. Customs and Immigration. Other calls were for tech support scams and loans that were supposedly pre-approved.

In the Global Voicecom case, the calls involved SSA, IRS and Treasury, USCIS, jury duty, tech support and calls supposedly from foreign governments, claiming problems with the immigration status or passport of people in the U.S.

## Fake caller ID or caller ID spoofing

Many people now have caller ID, which is meant to let them know who is calling by displaying the phone number and sometimes the name of the caller. But scammers are able to display any information they want. There have been calls that pretended to be from Social Security, the Competition Bureau in Canada, or local police. The SSA has now worked with the telephone industry to prevent their numbers from being displayed on caller IDs.

## Non-standard payment methods to scammers

There is no point in running a scam unless you can get money from victims. Most impostor scams get money through gift cards or stored value cards. At times, though, they have asked victims to do bank-to-bank wire transfers, use MoneyGram or

Western Union, or even ask for payment in bitcoin. What these payment mechanisms have in common is that it is very difficult to stop the transaction after victims realize that they have been defrauded.

**Gift cards:** This is the government impostor's favorite payment method. Scammers sometimes stay on the phone while victims drive to Walmart, Target or a pharmacy. After victims pay for the cards, the scammers tell them to read (or text a photo) of the codes on the back of the cards. Armed with this information, scammers can cash out the cards through a variety of websites. TIGTA also reports that many of the scammers use the gift cards to purchase phones or other electronics, which they then resell on online marketplaces. Both TIGTA and the SSA Inspector General (SSA IG) have been working with major retailers to educate them about scams and how to help victims that come in to buy these cards.

**Stored value cards:** Scammers sometimes use stored value cards such as those offered through Green Dot. The scammers have someone set up an online account, and the scammer has a physical card that can operate like an ATM card. Green Dot has a simple method to load more money onto these cards. Retail stores sell MoneyPaks in different denominations. Customers pay cash for these, which are simply pieces of cardboard, and the store enters the information into a computer system. Scammers then have victims scratch off the code on the card and read it to them. The scammers can then enter that information into their account online and then withdraw cash from ATM machines. Other companies offer stored value cards that operate essentially the same way.

**Other payment methods:** TIGTA says some scammers have victims send cash by Federal Express or UPS. Others open accounts at banks such as Bank of America, then ask victims to go to a local branch and deposit money into those accounts.

**Mules/runners:** Scammers need people in the U.S. or Canada to collect and launder the money sent by victims. They typically take the money out in cash, keep part of it as payment, and send the rest to India. Laundering money this way can be a complicated process. Law enforcement in the U.S. and Canada have successfully traced the money to Indian nationals in these countries and prosecuted them.

## Call center expertise

Most government impostor scams claiming to be from the SSA, the IRS, U.S. Customs, jury duty, and Medicare appear to originate from call centers in India. As a [previous BBB study](#) demonstrates, India is also home to most tech support scams.

**Why India?** India is a very large country with an educated populace but a great deal of poverty. English speakers are common, and many large companies use legitimate call centers there to handle customer service calls from the U.S. and Canada. Therefore, the country already has a sizable workforce trained in telemarketing. The same scams hitting the U.S. and Canada are also common in the [UK](#) and [Australia](#). The [BBC has aired](#) a video of the inside of a call center in India operating a tech support scam.



# LAW ENFORCEMENT EFFORTS TO COMBAT IMPOSTOR SCAMS

## Law enforcement efforts in the U.S. and Canada

Prosecuting impostor scammers has been a priority for law enforcement. Many Indian nationals have been living in the U.S. and Canada, sometimes illegally, while working directly with scam call centers in India. Many of these scammers received and laundered money from victims.

[TIGTA relates that 170 people](#) in the U.S. have been charged in federal court over IRS impostor scams. BBB has been able to identify [91 people prosecuted](#) to date in the United States. Most of those sentenced to date have received substantial sentences in federal court. Some face deportation when their prison term ends.

Some of these prosecutions have been the result of concentrated efforts and headed up in locations like the

Northern District of Georgia (Atlanta) and the Southern District of Texas (Houston). A sample of these include:

- October 2016: [Indictments of 61](#) for IRS impersonation from India in Southern District of Texas
- July 20, 2018: [24 defendants sentenced in India-based call center](#) scam in the Southern District of Texas
- September 7, 2018: [15 defendants and five India-based call centers](#) indicted over IRS impersonation
- March 12, 2019: [Three defendants and an India-based call center](#) indicted in the Northern District of Georgia

The Royal Canadian Mounted Police in Canada also prosecuted those handling the money for impostor frauds, including scammers in the [Toronto area](#) and in [British Columbia](#).

## Law enforcement efforts in India

Unfortunately, there is little evidence that the government of India has been able to stop the scammers. In several cases, the police there have taken part in raids on large call centers and arrested large numbers of people, but actual prosecutions are very rare. Corruption is clearly a problem. One IRS impersonator, with an interview posted on [YouTube](#), asserts that the call centers receive warnings in advance about police raids.

U.S. and Canadian law enforcement have worked with law enforcers in India who have “busted” a number of call centers located there. These include:

- In October 2016, [nine call centers](#) running an IRS scam that employed more than 770 people in Mumbai.
- In February 2018, a [call center in Pune](#) making IRS calls.
- In August 2018, a [call center in Bhayandar](#) impersonating IRS officials.
- In October 2018, a [call center in Noida](#) scamming Canadians by impersonating the Canadian Revenue Agency.

- In December 2018, [another call center in Noida](#) impersonated SSA employees and arrested 126 people.
- Between December 2018 and March 2019, the RCMP worked with India to bust [40 call centers](#) impersonating the Canada Revenue Agency.

Despite these efforts, there is little evidence that these scammers are being prosecuted in India. BBB has seen no signs that anyone has ever been extradited for prosecution.

A Justice Department official wrote an [article about efforts to fight telemarketing fraud](#) coming from India, saying:

To date, the United States government has not received any information concerning the investigation, arrest or prosecution by Indian authorities of 31 of the India-based defendants charged as part of the public indictment in this case for their alleged criminal conduct. The one and only defendant in this case known to have been prosecuted in India in relation to his involvement in similar Indian call center fraud, hailed in the Indian press as a “mastermind” of these schemes, was released from an Indian jail on bail after only 14 months of incarceration. See Arvind Walmiki, After 14 Months, Thane Call Centre Scam mastermind ‘Shaggy’ Granted Bail, HINDUSTAN TIMES (June 19, 2018).

## Not all impersonation calls come from India.

In January 2020, DOJ announced [prison sentences](#) for three men who had worked at a call center in Costa Rica. Callers pretended to be federal judges or FTC employees and told victims they had won a lottery and needed to pay a fee to receive their winnings. The scheme took in \$11 million. In addition, [more than 50 people have been prosecuted](#) for operating jury duty scams from prisons in Georgia. DOJ also has [prosecuted a massive operation](#) that used call centers in the Philippines, the Dominican Republic and Central America to impersonate Medicare in sales of unneeded back braces and other medical equipment.

# WHERE TO COMPLAIN ABOUT IMPOSTOR SCAMS

**IRS:** The IRS advises people to fill out the “IRS Impersonation Scam” form on TIGTA’s website, [tigta.gov](https://www.tigta.gov), or call TIGTA at 1-800-366-4484.

**Social Security:** SSA IG has its own [online form](#) to take complaints about frauds impersonating the SSA.

**Canadian Anti-Fraud Centre:** In Canada, contact CAFC about all government impersonation scams at 1-888-495-8501 or [online](#).

**Federal Trade Commission:** 877-FTC-Help or [ftc.gov](https://www.ftc.gov).

**Internet Crime Complaint Center:** <https://www.ic3.gov/complaint/splash.aspx>.

**Contact your cellphone carrier,** which may offer [free services](#) such as scam call identification and blocking, ID monitoring, a second phone number to give out to businesses so you can use your main number for close friends or a new number if you get too many spam calls.

File a report with **BBB** [Scam Tracker](#).

**E**rin is retired and lives in Wichita Falls, Texas. She received a phone call that woke her up early in the morning in December 2019. The caller claimed to be with Social Security and informed her there was a warrant out for her arrest for drugs and money laundering in El Paso, Texas. She said the caller stressed she needed to get dressed, go to Walmart to get a Walmart money card or she would be arrested. She was scared.

The caller said two federal agents would come to her house later to return the money and give her a new Social Security card. They stayed on the phone with her for nearly two hours as she drove to Walmart, purchased a \$500 money card with her MasterCard debit card, scratched off the number and read it to them.

Erin said as soon as she hung up, a light bulb went off and she realized this was probably a fraud. She called BBB and the credit union that issued her MasterCard, which refunded her money.



## Recommendations

- Efforts to prevent fraud calls to the U.S. and Canada have shown promising results, and the telecom industry should continue efforts to stop illegal calls and to end caller ID spoofing. Legislation may be needed to address the problem of gateway carriers.
- The government of India should do more to prosecute and extradite those operating frauds from that country.
- Law enforcement should continue to take action against scammers who are physically present in the U.S. and Canada.
- Efforts by many retailers and banks to question people buying gift cards have had limited success in stopping the purchase of gift cards to pay scammers. The gift card industry and retailers should explore additional ways to stem fraudulent use of their products.





**BBB International Investigations Initiative**

BBB Chicago [bbbinfo@chicago.bbb.org](mailto:bbbinfo@chicago.bbb.org)

BBB Dallas [info@nctx.bbb.org](mailto:info@nctx.bbb.org)

BBB Omaha [info@bbbinc.org](mailto:info@bbbinc.org)

BBB San Francisco [info@bbbemail.org](mailto:info@bbbemail.org)

BBB St.Louis [bbb@stlouisbbb.org](mailto:bbb@stlouisbbb.org)

**BBB International Investigations Specialist**

C. Steven Baker [stbaker@bbbinc.org](mailto:stbaker@bbbinc.org)